GFI EventsManager 8.2

Manual

By GFI Software Ltd.

http://www.gfi.com
E-mail: info@gfi.com

This manual was produced by GFI Software Ltd. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI Software Ltd.

GFI EventsManager is developed by GFI Software Ltd. GFI EventsManager is copyright of GFI Software Ltd. © 2000-2009 GFI Software Ltd. All rights reserved.

GFI EventsManager 8.2 - Last updated 8 January 2010

Version number: ESM-UM-EN-1.0.2

Contents

1 Introduction 1

1.1 About this manual 1
1.2 About GFI EventsManager 4
1.3 Key Features 5
1.4 How does GFI EventsManager work? 8
1.5 Operational privileges 9
1.6 Navigating the GFI EventsManager management console 10

2 Installation 11

2.1 Introduction 11
2.2 Managing Microsoft Windows Vista or later events 13
2.3 Hardware requirements 14
2.4 Software requirements 14
2.5 Upgrading from a previous version 14
2.6 Installation procedure 15

3 Getting Started 19

3.1 Introduction 19
3.2 Getting started: Running GFI EventsManager for the first time 22
3.3 Step 1: Configure the database backend 23
3.4 Step 2: Launch events processing 24
3.5 Step 3: Analyze events and generate reports 26

4 Event browsing 29

4.1 Introduction 29
4.2 Accessing and browsing stored event logs 33
4.3 Applying event queries 33
4.4 Creating custom event queries 34
4.5 Customizing the event viewer pane 36
4.6 Configuring event color coding 37
4.7 Event finder tool 38
4.8 Export events tool 39
4.9 Backup events 40
4.10 Switching databases 40
4.11 Clear all events 40

5 Generating reports 43

5.1 Introduction 43
5.2 Download the GFI EventsManager ReportPack 43
5.3 Launching the GFI EventsManager ReportPack 44

6 Customizing event sources 46

6.1 Introduction 46
6.2 Adding new event sources to the computers group 46
6.3 Configuring event source properties 47
6.4 Adding a new SQL Servers group 52

6.5 Configuring SQL Servers event source properties 52
6.6 Adding new SQL Servers to the default group 53
6.7 Removing SQL Servers from the default group 55
6.8 Configuring database server properties 55

7 Configuring event processing rules 57

7.1 Introduction 57
7.2 Collecting and processing Windows events 59
7.3 Configuring custom event logs 63
7.4 Collecting and processing W3C logs 64
7.5 Collecting and processing Syslogs 65
7.6 Configuring the Syslog server communications port 68
7.7 Collecting and processing SNMP Traps 70
7.8 Configuring the SNMP Trap server settings 72
7.9 Archiving events 73
7.10 Selecting event processing rules 74
7.11 Triggering event source scanning manually 75

8 Customizing event processing rules 77

8.1 Introduction 77
8.2 Create a new rule-set folder 78
8.3 Renaming and deleting folders 78
8.4 Creating a new rule-set 78
8.5 Editing a rule-set 79
8.6 Deleting a rule-set 79
8.7 Creating a new Windows Event Log rule 80
8.8 Creating a new W3C rule 82
8.9 Creating a new Syslog rule 85
8.10 Creating a new SNMP Trap rule 87
8.11 Creating a new SQL Server audit log 89
8.12 Changing the configuration settings of a rule 92
8.13 Advanced event filtering parameters 94

9 Customizing alerts and actions 95

9.1 Introduction 95
9.2 Configuring default classification actions 96
9.3 Configuring actions through event processing rules 97
9.4 Configuring alerting options 97

10 Configuring users and groups 103

10.1 Introduction 103
10.2 Configuring the administrator account 103
10.3 Creating a new user 109
10.4 Changing user properties 110
10.5 Deleting users 110
10.6 Configuring groups 111
10.7 Enabling and disabling the GFI EventsManager login system 113
10.8 Enabling and disabling user action auditing 114

11 Status monitoring 117

11.1 Introduction 117
11.2 Accessing the status monitor 117
11.3 General status view 118
11.4 Job activity view 121
11.5 Statistics view 124

12 Database Operations 127

12.1 Introduction 127
12.2 Why is there a need for database maintenance? 127
12.3 Configuring Database Operations 128
12.4 Creating maintenance jobs 131
12.5 Move to database 133
12.6 Export to file 134
12.7 Import from file 136
12.8 Delete data 138
12.9 Configuring data filter conditions 139
12.10 Viewing scheduled maintenance jobs 142
12.11 Editing a maintenance job 142
12.12 Changing maintenance job priority 144
12.13 Deleting a maintenance job 144

13 Miscellaneous 145

13.1 Command line operations 145
13.2 Product licensing 147
13.3 Version information 148

14 Troubleshooting 150

14.1 Introduction 150
14.2 Knowledge Base 150
14.3 Web Forum 150
14.4 Request technical support 150
14.5 Build notifications 151

Index 153

1 Introduction

1.1 About this manual

1.1.1 How is this manual structured

This manual is structured in line with the logical chain of configuration operations required to get GFI EventsManager up and running.

Chapter 1 gives an overview of how GFI EventsManager works.

Chapter 2 explains how to run GFI EventsManager for the first time, including how to configure the database backend and how to process event logs for the first time.

Chapter 3 describes how to use the built-in events browser to analyze events stored in the GFI EventsManager database backend. This chapter explains how to use the tools and features provided in the events browser including:

- Default event log queries and custom query builder
- Event color-coding
- Event finder tool.

Chapter 4 describes how to enable the GFI EventsManager ReportPack to create reports that further analyze the events stored in the GFI EventsManager database backend.

Chapters 5, 6, 7 and 8 guide you through the process of customizing essential parameters required for event processing. At the end of these chapters, you will be able to customize:

- Event sources that will be monitored (e.g. SQL Server)
- Log-types that will be collected and processed (Windows events, W3C, Syslog, SNMP Traps
- Configuring and customizing event processing rules
- Alerts and actions that will be triggered on key events

Chapter 9 describes how to configure alert recipient parameters including:

- Personal details such as mobile phone number
- Normal working hours
- Type of alerts that will be sent to every recipient.

Chapter 10 describes how to analyze the status of GFI EventsManager as well as view statistical information and processed events.

Chapter 11 explains how to centralize events collected by other remote GFI EventsManager instances and how to optimize database backend performance.

Chapter 12 describes miscellaneous options such as command line operations and licensing.

Chapter 13 explains what main sources of information are available to help users troubleshoot product issues.

1.1.2 Glossary of terms used in this manual

Actions	The activity that will be carried out as a result to events matching specific conditions. For example you can trigger actions whenever an event is classified as critical. Actions supported by GFI EventsManager include Email alerts, event archiving and execution of scripts.
Alerts	Notifications which inform recipients that a particular event has occurred. GFI EventsManager can generate Email alerts, SMS alerts and Network alerts.
Archive	A collection of events stored in the SQL Server based database backed of GFI EventsManager.
Email alerts	Email notifications which inform recipients that a particular event has occurred. To enable email alerts, you must have access to an active mail server.
Event classification	The categorization of events as Critical, High Medium, Low or Noise.
Event logs	A collection of entries which describe events that occurred on the network or on a computer system. GFI EventsManager supports different types of event logs including: Windows Event Log, W3C Logs, Syslog, SNMP Traps and SQL Server audit events.
Event processing rules	A set of instructions which are applied against an event log.
Management Information Base	A MIB is the equivalent of a data dictionary or codebook. It associates object identifiers (OIDs) with a readable label and various other parameters related to an active network object such as a router. Its main function is to assemble and interpret SNMP messages transmitted from SNMP-enabled network devices. The information stored in MIBs is organized hierarchically and is normally accessible using a protocol such as SNMP.
Network alerts	Network messages (known as Netsend messages) which inform recipients that a particular event has occurred. These messages are sent through an instant messenger system/protocol and are shown as a popup in the system tray of the recipient's desktop. To setup network alerts, you must specify the name or IP of the computers where the Netsend messages will be sent.
Noise	Repeated log entries which report the same event.

Rule-set folder	The folder which contains one or more rule-sets.
Rule-sets	A collection of event processing rules.
SMS alerts	SMS notifications which inform recipients that a particular event has occurred. In GFI EventsManager, SMS alerts can be sent through various sources including mobile phones with modem capabilities and email-to-SMS web-based gateways.
SNMP Object Identifier (OID)	An SNMP object identifier is an address made up of a sequence of 'dotted' numbers (e.g. 1.3.6.1.4.1.2682.1). These numbers uniquely identify and locate a specific device (e.g. hub) within the entire network. SNMP OIDs are a key component in the assembly of SNMP messages. In fact, an SNMP server cannot interpret or assemble messages which don't have an OID. Individual vendors often create their own MIBs that only include the OIDs associated specifically with their device.
SNMP Traps	Notifications/alerts generated and transmitted by active network components (e.g. hubs, routers and bridges) to SNMP server(s) whenever important events such as faults or security violations occur. Data contained in SNMP Traps may contain configuration, status as well as statistical information such as number of device failures to date.
Syslog messages	Notifications/alerts most commonly generated and transmitted to a Syslog server by UNIX and Linux-based systems whenever important events occur. Syslog messages can be generated by workstations, servers as well as active network devices and appliances such as Cisco routers and Cisco PIX firewalls to record failures and security violations amongst other activities.
Unclassified events	Events that did not satisfy any of the event processing conditions configured in the event processing rules.
W3C logs	W3C is a common log format developed by the World Wide Web Consortium. W3C logs are text-based flat files used mainly by web servers including Microsoft Internet Information Server (IIS) to record web related events such as web logs.
Windows Event Logs	A collection of entries which describe events that occurred on a computer system running Windows OS.

1.2 About GFI EventsManager

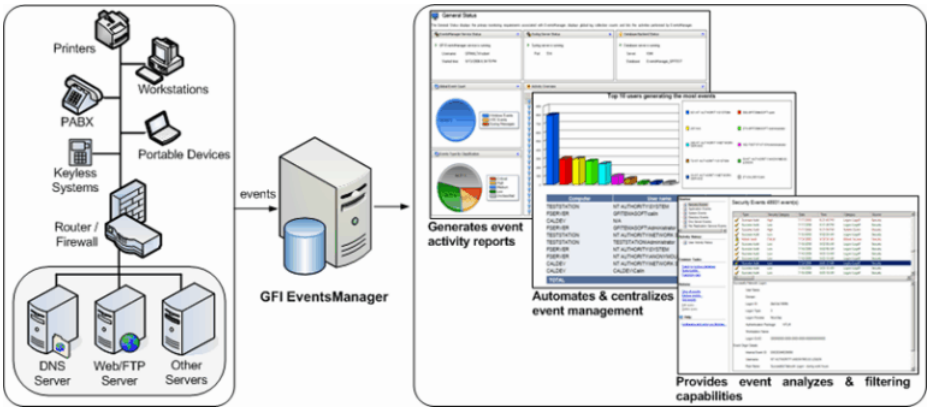


Figure 1 - GFI EventsManager integrates into any existing IT infrastructure

GFI EventsManager is a results oriented event log management solution which integrates into any existing IT infrastructure, automating and simplifying the tasks involved in network-wide events management.

Through the features supported by GFI EventsManager you can:

- Automatically collect W3C, Syslog, SNMP Traps and Windows events from network devices and Windows/Linux/Unix based systems and manage them through one console.
- Archive collected events in a centralized SQL Server based database backend for future analysis and forensic studies.
- Filter unwanted events and classify key events through the use of powerful default or custom-built event processing rules.
- Automate alerting and remedial actions such as the execution of scripts and files on key events.
- Monitor your network activity and the status of your GFI EventsManager scanning engine through a built-in graphical dashboard.
- Analyze events through a built-in events browser as well as export these events to CSV files for further processing and report customization.
- Simplify event forensics through specialized tools which include a built-in event query builder, an event finder tool and an event color-coding tool.
- Increase event processing power through a high-performance event scanning engine.
- Generate, schedule as well as email event activity and trend reports through GFI EventsManager ReportPack - the powerful reporting companion tool which ships by default with GFI EventsManager.
- Monitor the operational health status of your SQL Servers in real-time by processing the activity logs/messages generated by day-to-day SQL Server operations.

1.3 Key Features

Extended event log support

GFI EventsManager is able to process various event log types including Windows Event Logs, W3C logs, Syslog and SNMP Trap messages. This allows you to collect more data from the different hardware and software systems that are most commonly available on a typical corporate network. For a summary list of hardware and software systems that are supported by GFI EventsManager out of-the-box refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003302.

Rule-based event log management

GFI EventsManager ships with a pre-configured set of event processing rules that allow you to filter and classify events collected from a variety of event-log sources. You can run these default rules without performing any configuration or you can choose to customize these rules or create tailored ones that suite your network infrastructure. For a list of event-log sources that can be processed by GFI EventsManager out-of-the-box refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002868.

Event log scanning profiles

GFI EventsManager allows you to organize event log scanning rules into 'Scanning Profiles'. In a scanning profile, you can configure the set of event log monitoring rules that will be applied to a specific computer or group of computers. The benefits of these profiles include:

- The simplification product administration tasks by providing a centralized way of tuning event processing rules.
- Allowing administrators to create different sets of event log rules that suit the roles of scanned event sources and the corporate network environment. For example, you can setup a set of rules which apply only to workstations in a particular department.

Allow granular configuration of rules

Administrators can create an event processing profile that is generic for all computers and a number of separate profiles which complement the generic profile by providing additional and more specialized event log rules on a computer by computer basis.

Translates cryptic Windows events

One major drawback of Windows Event Logs is that they are not user friendly - too cryptic for the user to understand. In fact this is one of the main reasons why only few administrators really peer into Windows Event Logs. GFI EventsManager overcomes this problem by translating event descriptions into a way that is more users friendly and easier to understand.

Enhanced event scanning engine

GFI EventsManager includes an event scanning engine that has been tuned to effectively speed up event scanning for maximum performance. This engine adopts a plug-in based concept that allows the 'plugging-in' of additional features/modules without having to perform physical changes to the existing code - hence more stability without effecting scalability.

Automatic noise reduction

GFI EventsManager identifies and removes unwanted event data (such as noise and background process generated events) providing you with only the relevant, usable data. Hence facilitates event forensics by reducing the amount of events to be analyzed.

Enhanced real-time actions

GFI EventsManager can generate alerts or trigger actions such as script execution when key events are detected. You can alert one or more people in various ways including: email, network messages, and SMS notifications sent through an email-to-SMS gateway or service. Actions can be configured to trigger on event classification or by configuring specific conditions in event processing rules.

Advanced event filtering features

GFI EventsManager ships with a number of event filtering features including:

- **Pre-configured event queries and a custom event query builder:** The pre-configured event queries allow you to sift event log data and browse only the required events - without deleting any records from your database backend. The built-in event query builder allows you to create your own custom event queries.
- **Event color-coding capabilities:** Through this feature you can selectively color particular events in specific colors. This way during log browsing you can easily identify important events through their color.
- **Event finder tool:** With this tool you can quickly locate important events by providing specific search criteria such as event type.

Event centralization

GFI EventsManager enables you to monitor and manage events generated by Windows\Linux\Unix systems, network devices and software applications through a single user console.

User access privileges

GFI EventsManager allows you to assign management console access privileges on a user-by-user basis. This means that you can allow specific users to access the GFI EventsManager console for event-browsing only and at the same time allow other more privileged users to access and change the GFI EventsManager configuration settings.

SQL Server audit

GFI EventsManager allows you to automatically monitor the operational health status of your SQL Servers. This is achieved by processing in real-time the activity logs/messages generated by day-to-day SQL Server operations. SQL server activity that is monitored includes server startup, login activity, backups, server-side traces and more. Additionally, GFI EventsManager can also alert you via email, network or SMS notifications on key events like server shutdown and consecutive failed logins.

Database operations (WAN Connector)

The Database Operations module allows you to collect events data from GFI EventsManager installations on multiple sites and locations across your network into a central database. This add-on integrates and centralizes events collected and processed and allows you to backup/restore events on demand. Through Database Operations you can manage the size of the database - without the need for manual intervention - not only through centralization but by also being able to export events and back them up as needed.

Management Information Base

Management Information Base (MIBs) contain definitions and device information that are provided by device manufacturers. GFI EventsManager ships with MIB definitions for the following vendors: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis and others. GFI EventsManager also allows you to edit the MIB tree.

1.4 How does GFI EventsManager work?

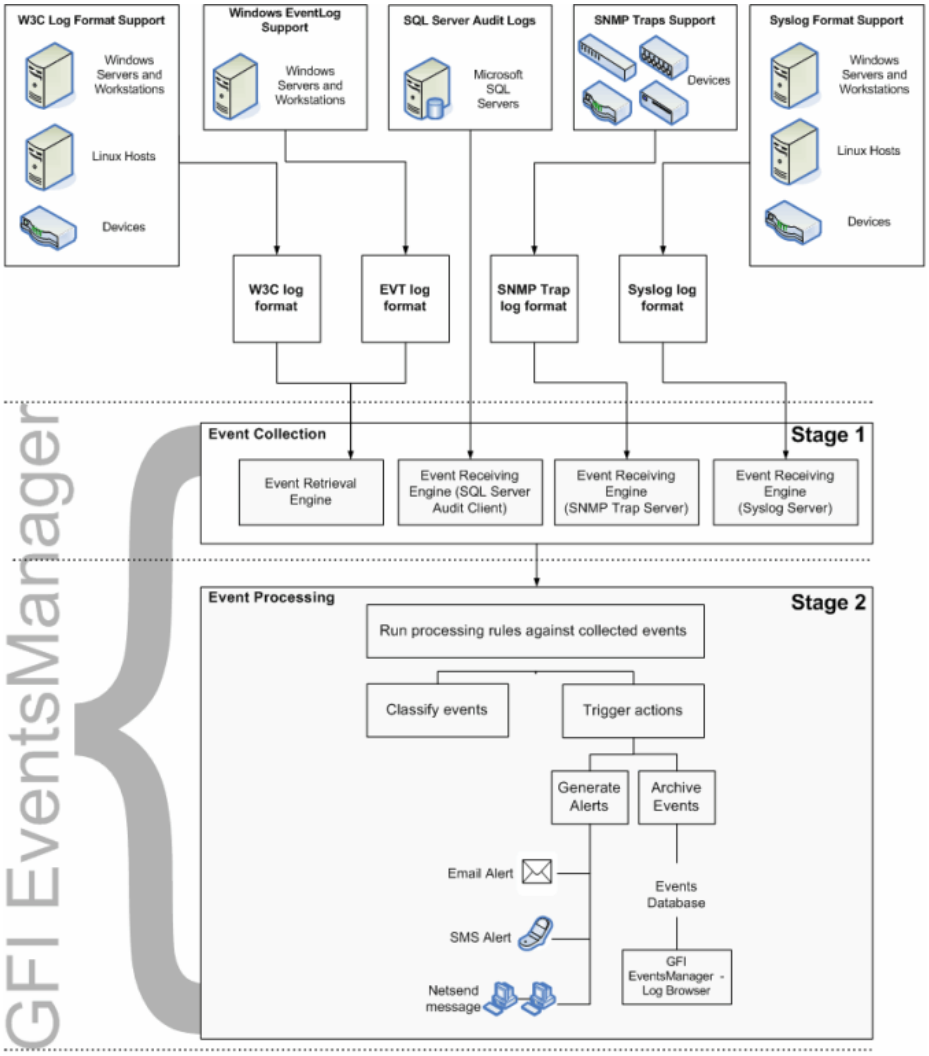


Figure 2 - The GFI EventsManager operational stages

The operational functionality of GFI EventsManager is divided into 2 stages:

- **Stage 1: Event Collection**
- **Stage 2: Event Processing**

A description of every stage is provided below.

Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of 2 event collection engines: The Event Retrieval Engine and the Event Receiving Engine.

The Event Retrieval Engine - The Event Retrieval Engine is used to collect Windows Event Logs and W3C logs from networked event sources. During the Event Collection process this engine will:

1. Log-on to the event source(s)
2. Collect events from the source(s)

3. Send collected events to the GFI EventsManager Server

4. Log-off from the event source(s).

The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console.

The Event Receiving Engine - The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured.

By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are however customizable via the GFI EventsManager management console.

Stage 2: Event Processing

During this stage, GFI EventsManager will run a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

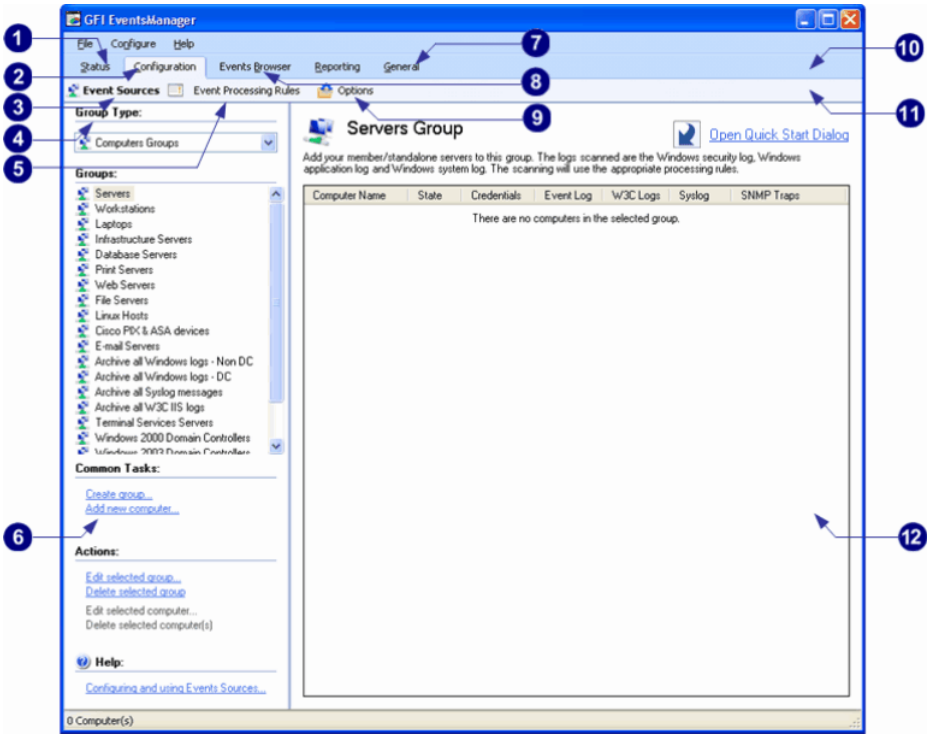
- Analyze the collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- Filter events that match specific conditions
- Trigger email, SMS and network alerts on key events
- Trigger remediation actions such as the execution of executable files or scripts on key events
- Optionally archive collected events in the database backend.

GFI EventsManager can be configured to archive events without running Event Processing rules. In such cases, even though no rules will be applied against collected logs, archiving will still be handled by the Event Processing stage.

1.5 Operational privileges

Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to: http://kbase.gfi.com/showarticle.asp?id=KBID001122.

1.6 Navigating the GFI EventsManager management console



Screenshot 1 - The GFI EventsManager management console

1. **Status option** - Use this option to view the status of GFI EventsManager and statistical information on processed logs.
2. **Configuration option** - Use this option to access and configure the main event processing options.
3. **Event Sources** - Use this option to configure event sources including which logs to collect and which rules to process.
4. **Group Type** - Use this drop-down to switch between event log source groups (i.e. Computer and Database Servers Groups).
5. **Event Processing Rules** - Use this option to create, configure and customize event processing rules.
6. **Left pane** - Use this pane to navigate through the additional configuration options provided in GFI EventsManager.
7. **General options** - Use this option to check for product updates, as well as view version and licensing details.
8. **Events Browser** - Use this option to browse the events stored in the GFI EventsManager database backend.
9. **Options** - Use this option to configure general settings such as database backend and default alerting parameters.
10. **Tabs Bar** - Use the tabs provided in this bar to access all primary configuration tab options.
11. **Tab options** - Use the Tab options to access and configure GFI EventsManager operational parameters.
12. **Right pane** - Event browsing and parameter configuration pane.

2 Installation

2.1 Introduction

Where can I install GFI EventsManager on my network?

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network.

Use GFI EventsManager to manage the events generated:

- On the same computer where it is installed
- On all the computers that are reachable from the computer on which it is installed.

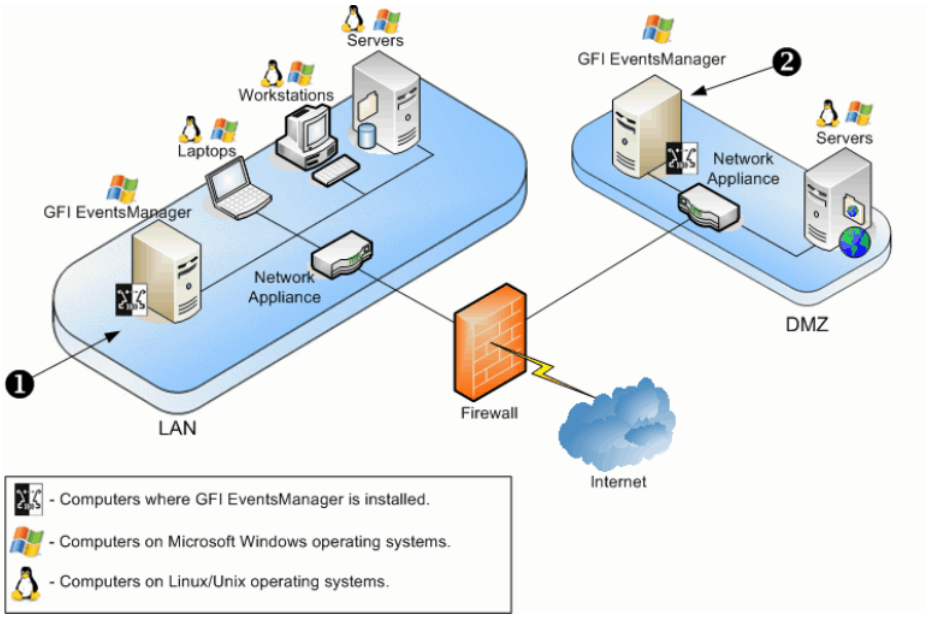


Figure 3 - GFI EventsManager deployment scenario

GFI EventsManager can be deployed:

1. Within your network to monitor the activity of internal servers and workstations/end points.

2. On the DMZ to monitor and manage the events generated on your servers.

2.1.1 Deployment of GFI EventsManager on a local area network

GFI EventsManager can be deployed on Windows based networks as well as on mixed environments where Linux and UNIX systems are being used as well.

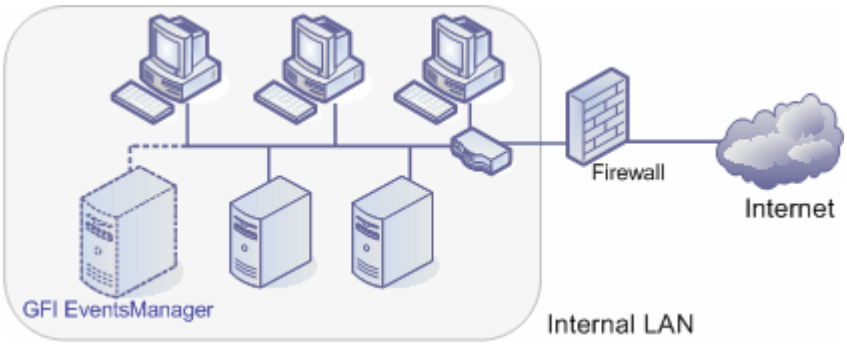


Figure 4 - Deployment of GFI EventsManager on LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows events, W3C event logs, Syslog messages, SNMP Trap and SQL Server audit messages generated by any hardware or software that is connected to the LAN, including:

- Workstations and Servers (e.g. Apache web-servers)
- Network appliances (e.g. Cisco PIX firewalls)
- Third party software (e.g. GFI EndPointSecurity)
- Specialized Services (e.g. Microsoft Internet Information Server - IIS)
- PABXs, Keyless Access Systems, Intrusion detections systems, etc.

When installed on a LAN, GFI EventsManager can also be used to collect events from hardware and software systems deployed on a Demilitarized Zone (DMZ). Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

1. The communication ports used by GFI EventsManager are not blocked by the firewall. For more information on the communication ports used by GFI EventsManager refer: http://kbase.gfi.com/showarticle.asp?id=KBID002770.

2. That GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

2.1.2 Deployment of GFI EventsManager on a demilitarized zone

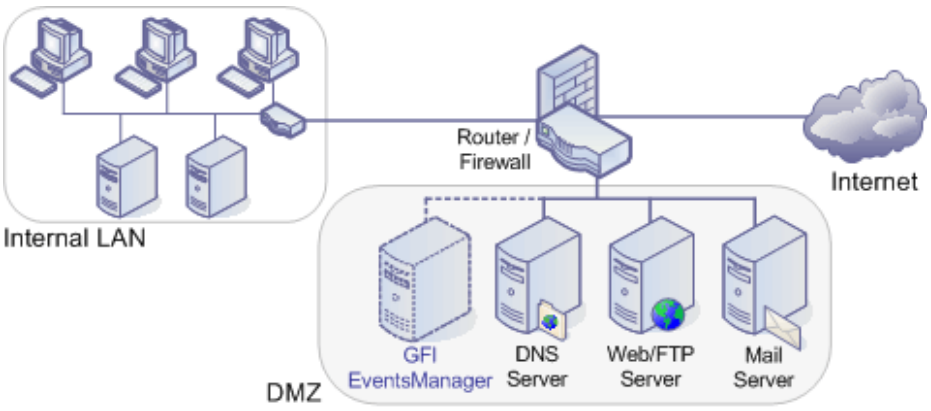


Figure 5 - The DMZ sits between the internal LAN and the Internet

GFI EventsManager can also be deployed on a Demilitarized Zone (DMZ). This is the neutral network which sits between the “internal” corporate network and the “outside world” (i.e. the internet). The deployment of GFI EventsManager on a DMZ helps you automate the management of events generated by DMZ hardware and software systems.

Automate management of Web and Mail server events

DMZ networks are normally used for the running of hardware and software systems that have internet specific roles such as HTTP servers, FTP servers, and Mail servers.

Hence, you can deploy GFI EventsManager to automatically manage the events generated by:

- Linux/Unix based web-servers including the W3C web-logs generated by Apache web-servers on LAMP web platforms.
- Windows based web-servers including the W3C web-logs generated by Microsoft Internet Information Servers (IIS).
- Linux/Unix and Windows based mail-servers including the Syslog ‘auditing services’ messages generated by Sun Solaris v. 9 or later.

Automate management of DNS server events

If you have a public DNS server, there’s a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically collect and process DNS server events including those stored in your Windows’ DNS Server logs.

Automate management of network appliance events

Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (e.g. Cisco IOS series routers) not only help protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can augment the operational performance of your systems.

By deploying GFI EventsManager on your DMZ, you can collect the events generated by such network appliances. For example, you can configure GFI EventsManager to act as a Syslog Server and collect in real-time the Syslog messages generated by Cisco IOS routers.

2.2 Managing Microsoft Windows Vista or later events

Microsoft Windows Vista, Microsoft Windows 7 and Windows Server 2008 introduced extensive structural changes in event logging and event log management mechanisms. The most important of these changes include:

- A new XML-based format for event logs. This provides a more structured approach to reporting on all system occurrences.
- The introduction of event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- A new file format (evtx) that replaces the old evt file format.

NOTE: To collect and process event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a system running Microsoft Windows Vista or later.

2.3 Hardware requirements

- Processor: 2.5 GHz or higher processor clock speed
- RAM: 1024 MB
- Hard disk: 2 GB of available space

NOTE: Hard disc size depends on your environment, the size specified in the requirements is the minimum required to install and archive events.

2.4 Software requirements

Software requirements - Installation machine(s)

Supported Operating Systems

- Windows Server 2008 - Standard or Enterprise (x86 or x64)
- Windows Server 2008 R2 - Enterprise
- Windows Server 2003 (SP2) - Standard or Enterprise (x86 or x64)
- Windows 2000 (SP4) - Server or Advanced Server
- Windows 7 - Enterprise, Professional or Ultimate (x86 or x64)
- Windows Vista - Enterprise, Business or Ultimate (x86 or x64)
- Windows XP - Professional (x86 or x64)
- Windows SBS 2008
- Windows SBS 2003

Other components

- .NET framework 2.0 or later.
- Microsoft Data Access Components (MDAC) 2.8+ or later

Software requirements - Scanned machine(s)

- For Microsoft Windows event log scanning:
  - Remote registry service must be enabled.
- W3C log scanning:
  - The source folders must be accessible via Windows shares.
- Syslog and SNMP Traps:
  - Sources/senders must be configured to send messages to the computer/IP address where GFI EventsManager is installed.

2.5 Upgrading from a previous version

Upgrading from version 7.0 or version 7.1 of GFI EventsManager to GFI EventsManager version 8.2 is fully supported. To upgrade to GFI EventsManager 8.2, follow the installation procedures provided in the installation procedure section within this chapter of the user manual.

Upgrading from versions older than version 7 is not possible due to the underlying operational and processing technology subsystems

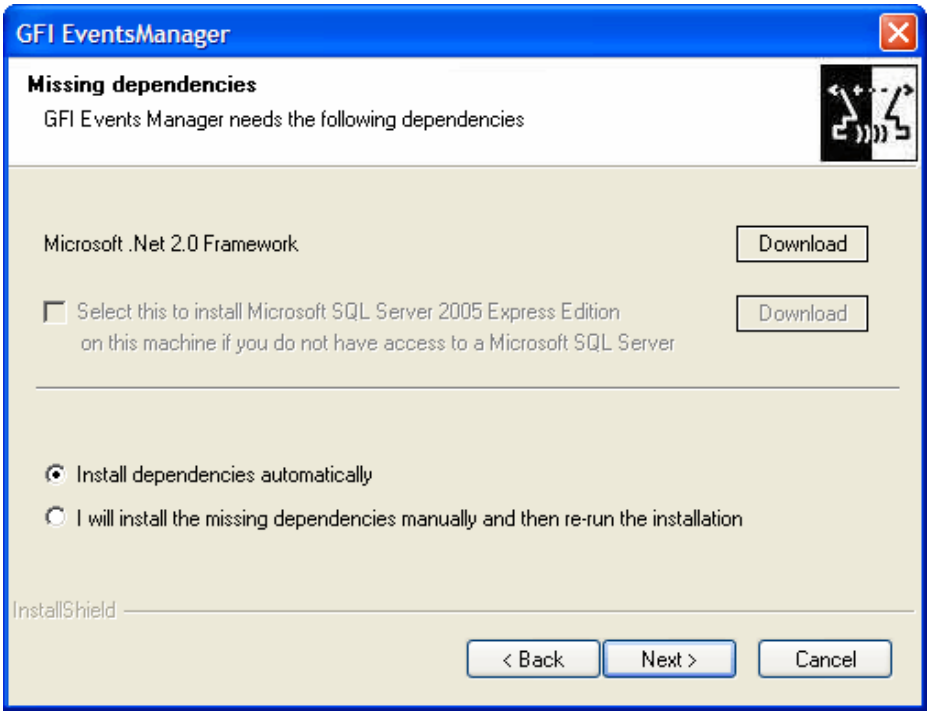
which are different from the current version of GFI EventsManager. You will still however be able to run an older (pre-version 7) version of GFI EventsManager on the same machine on which a newer version of GFI EventsManager is installed since there are no conflicts between the older and the newer versions.

2.6 Installation procedure

GFI EventsManager includes an installation wizard which will assist you through the installation process. To start the installation:

1. Close all running applications and log-on the target computer using an account which has local administrative privileges.

2. Double-click on **eventsmanager8.exe**.

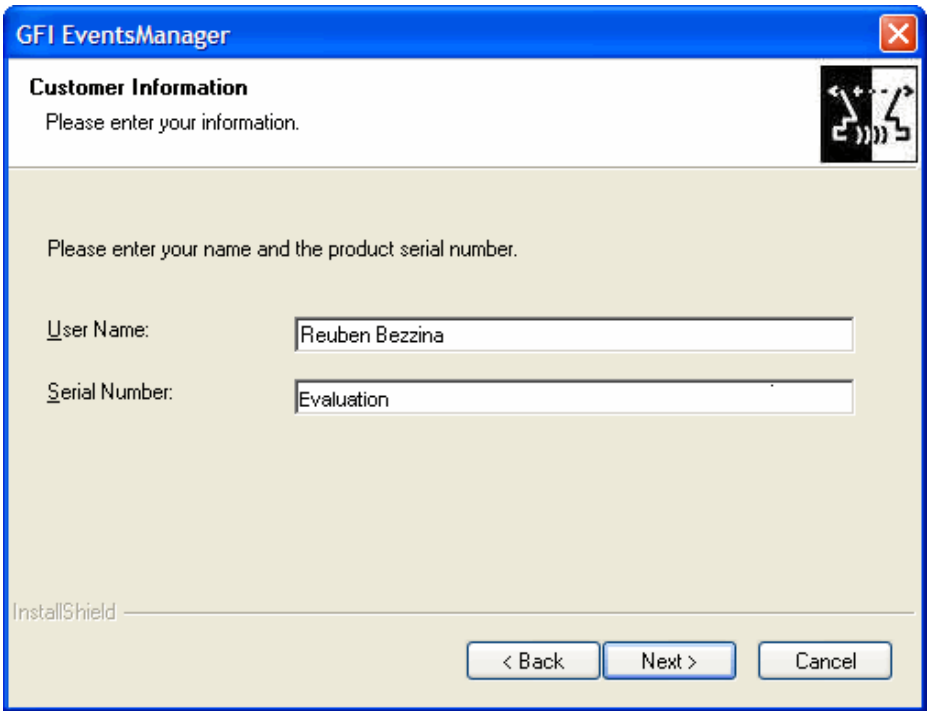

GFI EventsManager
Missing dependencies
GFI Events Manager needs the following dependencies
Microsoft .Net 2.0 Framework
Download
Select this to install Microsoft SQL Server 2005 Express Edition on this machine if you do not have access to a Microsoft SQL Server
Download
Install dependencies automatically
I will install the missing dependencies manually and then re-run the installation
InstallShield
< Back
Next >
Cancel

Screenshot 2 - Missing dependencies dialog

3. If GFI EventsManager detects that the basic dependencies are not present, a dialog will outline the missing dependency or dependencies and you will be allowed to install the missing dependencies manually or automatically.

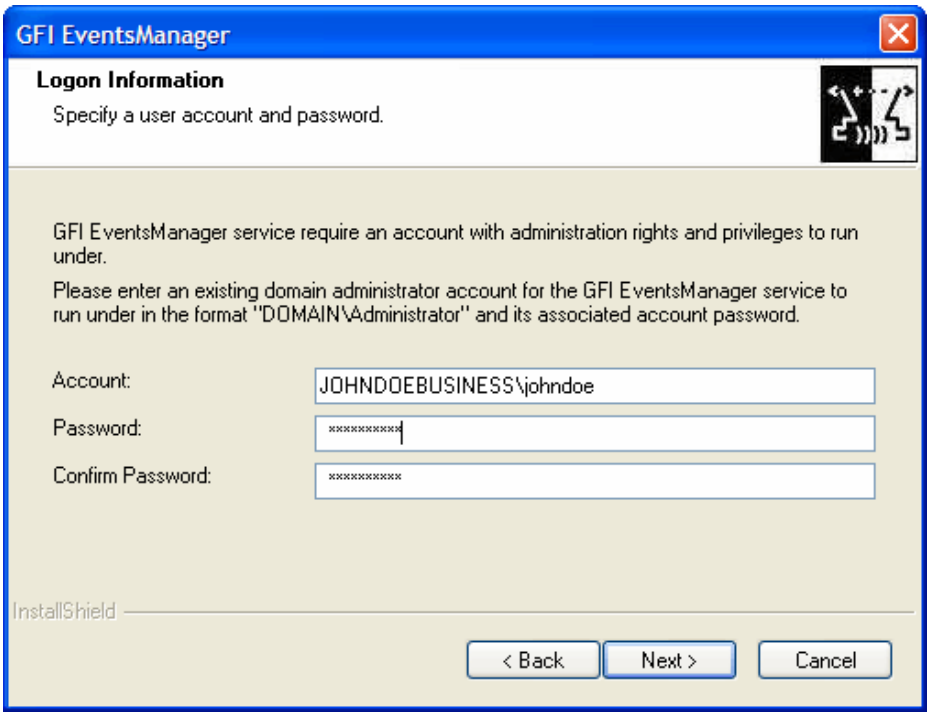
4. As soon as the welcome dialog is displayed, click **Next** to start the installation.

5. Read the licensing agreement carefully. To continue installing the product, select the '**I accept the Licensing agreement**' option and click **Next**.



Screenshot 3 - Customer and License detail screen

6. Specify your name and license key. If you are evaluating the product, leave the license key as default (i.e. '**Evaluation**') and click **Next**.


GFI EventsManager
Logon Information
Specify a user account and password.
GFI EventsManager service require an account with administration rights and privileges to run under.
Please enter an existing domain administrator account for the GFI EventsManager service to run under in the format "DOMAIN\Administrator" and its associated account password.
Account:
JOHNDOEBUSINESS\johndoe
Password:
Confirm Password:
InstallShield
< Back
Next >
Cancel

Screenshot 4 - Logon information screen

7. GFI EventsManager must run under an account which has domain administrative privileges. Enter the user name and password of domain administrator account and click **Next** to continue.

8. Specify an alternative installation path or click on **Install** to leave as default and proceed with the installation.

9. Click **Finish** to finalize the installation.

3 Getting Started

3.1 Introduction

What is a computer log?

A computer log is a collection of events entries. These entries provide an audit trail of information related to the activity of a network or computer system. In fact, computer logs are recorded in a certain scope to provide information suitable for forensic analysis. The computer log may be a binary file as in the case of Windows logs, or text-based files as in the case of Syslog or W3C logs.

What is a log?

An event is a log entry that provides information on something that occurred within a computer system or network. Such events include various details such as the date and time the event occurred and a related description. Event entries are often stored in chronological order to facilitate event browsing and forensic analysis.

What are Windows Event Logs?

Windows Event Logs are a systematic recording of computer related events that occurred within computer systems and networks running on Windows Operating Systems. In systems running on Windows 2000/XP/2003/VISTA, events are recorded and organized in 3 default event logs:

- **Application log**
- **Security log**
- **System log.**

Computers with specialized network roles such as domain controllers and DNS servers allow the logging of events to additional (default) logs such as:

- **Directory service log**
- **File Replication service log**
- **DNS server log.**

Windows Event Logs contain the following types of events:

Error - Error events indicate that a significant problem, such as loss of data or functionality has occurred. For example an Error event is recorded every time that a service or driver fails to load during startup.

Warning - Warnings indicate events that are not necessarily significant, but which may possibly cause future problems. For

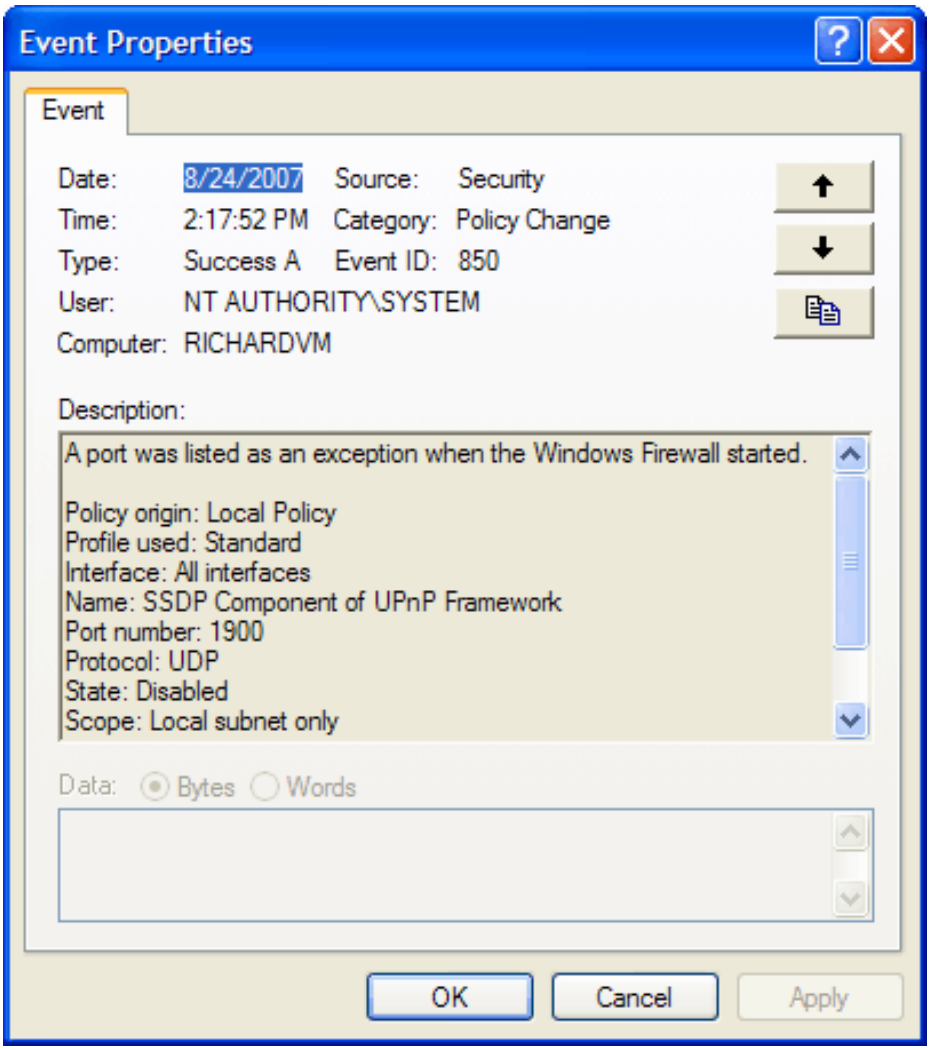
example, a Warning event is recorded every time that disk space runs low.

Information - Information events describe the successful operation of an application, driver, or service. For example, an Information event is recorded every time that a network driver loads successfully.

Success Audit - Success audit events indicate security access attempts that were successful. For example, a Success Audit event is recorded every time that a user successfully logs on to his Windows based workstation.

Failure Audit - Failure audit events indicate security access attempts that failed. For example, a Failure audit event is recorded every time that a user fails to access a network drive.

A sample of the information typically recorded in a Windows Event Log is shown below.



Screenshot 5 - Windows event log

What are W3C logs?

W3C logs are used mainly by web servers to log web related events including web logs. W3C logs are recorded in text-based flat files using any one of the two W3C logging formats currently available:

- W3C Common Log file format
- W3C Extended Log File format.

The W3C common log file format was the first format to be released and to date it is still the default format used by a variety of popular web servers including Apache. There is however one downside - the information about each server transaction is fixed and does not provide for certain important fields such as referrer, agent, transfer time, domain name, or cookie information. To overcome this problem, the W3C Extended log file format was released. This newer type of log is in customizable ASCII text-based format, permitting a wider range of data to be captured. The W3C Extended log file format is the default log file format used by Microsoft Internet Information Server (IIS).

A sample of the information typically recorded in a W3C extended type log is shown below.

#Version: 1.0

#Date: 04-Sep-1996 00:00:00

#Fields: time cs-method cs-uri

00:34:23 GET /WebSRV/Pg_Snippet.html

12:21:16 GET /WebSRV/ Button_pg.html

12:45:52 GET /WebSRV/ Login_Pg.html

12:57:34 GET /WebSRV/ Error_msg.html

What are Syslogs?

Syslog is the standard for logging messages, such as system events, in an IP network. The Syslog standard is most commonly used for the logging of events by computer systems running on UNIX and Linux as well by network devices and appliances such as Cisco routers and the Cisco PIX firewall. Syslog events are not directly recorded by applications running on the computer systems. Whenever an event is generated, the respective computer will send a small textual message (known as Syslog message) to a dedicated server commonly known as 'Syslog server'. The Syslog server will then save the received message into a log file. Syslog messages are generally sent as clear text; however, an SSL wrapper can be used to provide for a layer of encryption.

Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, its big plus is that Syslog is supported by a wide variety of devices and receivers. Because of this, Syslog can be used to integrate log data from many different types of systems into a central repository using the Syslog server as a log aggregator.

The Syslog daemon handles the recording of Syslog messages/events in log files. The Syslog message is composed of two main parts:

1. The 'header' which contains date/time information as well as the IP or computer name from where the message has originated.

2. The "message" which includes the program or subsystem name and the message itself, separated by a colon.

The following is an example of a Syslog message:

Sep 4 10:10:10 10.245.2.11 foo[421]: this is a message from WebSRV

What are SNMP Traps?

SNMP Traps are used by network management systems to monitor network devices (such as routers, firewalls or switches) for conditions that require administrative attention. This includes monitoring device uptime, inventories of operating system versions and collecting interface information. SNMP enabled devices do not record event messages locally but instead these transmit event details to an SNMP Trap server which analyzes these occurrences and alert systems administrators on key events.

GFI EventsManager includes its own SNMP Trap server that captures SNMP messages and informs systems administrators of network device failures and other critical events. GFI EventsManager supports various versions of SNMP Traps including SNMP versions 1, 2 and 3 (the encoded version).

What are SQL Server audit logs?

Microsoft SQL Server generates event logs that allow the network administrator to monitor database activity. GFI EventsManager allows you to process the activity logs generated by day-to-day SQL Server operations such as server startup or on key events such as failed logons. Alerts can also be created when key events such as consecutive login failure is identified in Microsoft SQL Server audit logs.

3.2 Getting started: Running GFI EventsManager for the first time

After installation, the GFI EventsManager console is launched automatically. To launch GFI EventsManager click **Start ► All Programs ► GFI EventsManager 8.2► Management Console**.

Follow the steps outlined below to configure GFI EventsManager for first time use:

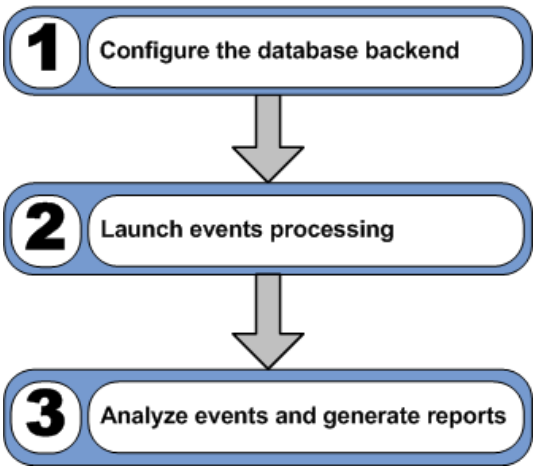
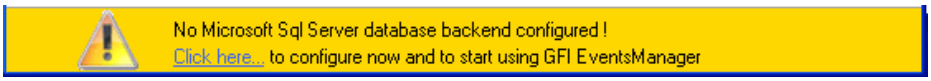


Figure 1: Running GFI EventsManager for the first time

3.3 Step 1: Configure the database backend

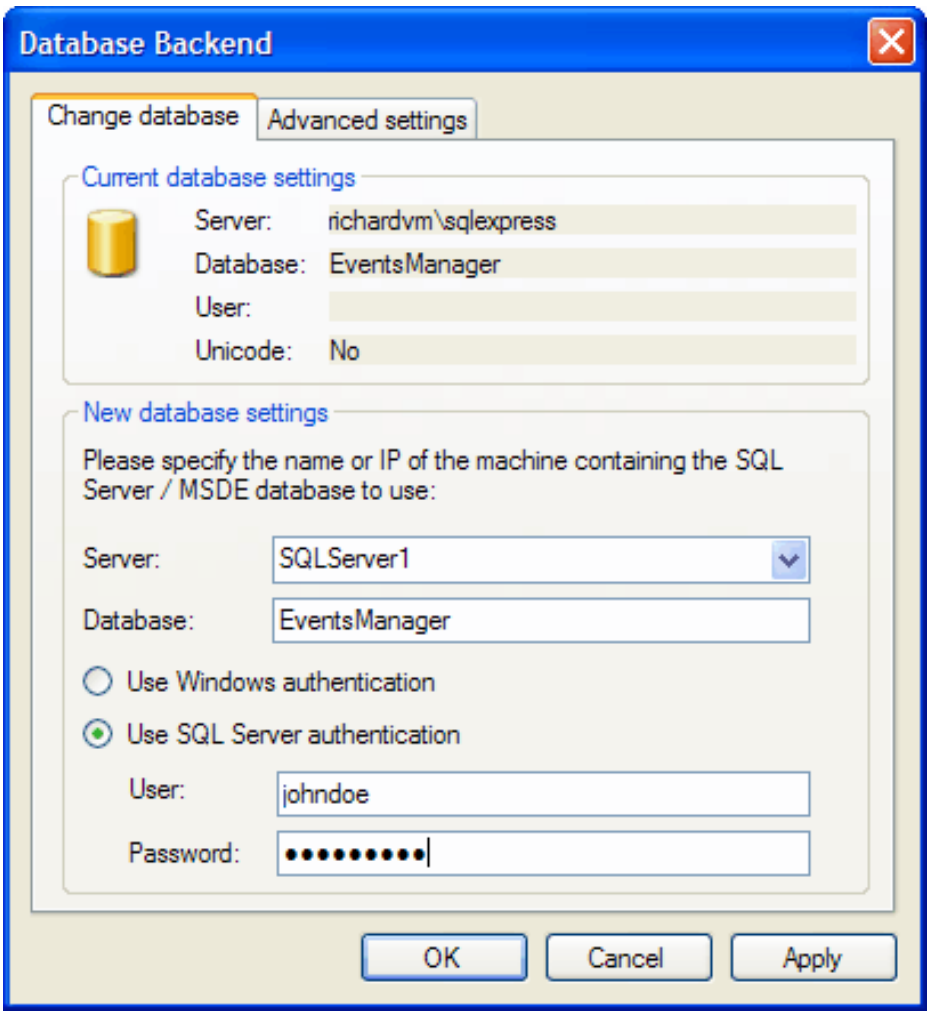
Set up the database backend on first launch of GFI EventsManager..

NOTE: If you opted to install Microsoft SQL Server during the GFI EventsManager installation, the database backend required by GFI EventsManager will be set up automatically. You are therefore not required to manually create the database backend.



Screenshot 6 - Database backend alert displayed on Quick Start Dialog

An alert will appear at the bottom of the Quick Start Dialog indicating that you are required to configure a Microsoft SQL Server database backend . Click on **Click here…** in the alert box to configure the Microsoft SQL backend database.



Screenshot 7 - Database Options - Change database tab

To configure the SQL Server and database backend details:

1. Specify the name/IP of your SQL Server.

2. Key in a name for your database backend (e.g. EventsManager).

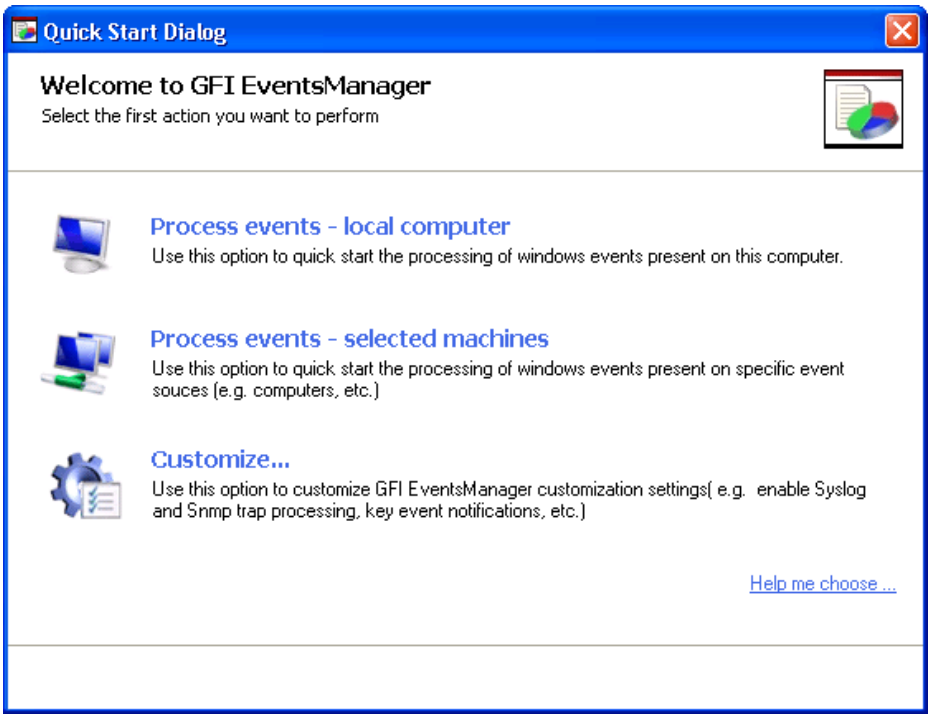
3. Select the authentication method used to connect to the SQL Server. If SQL Server authentication is selected, specify the login username and password.

4. Click **Advanced settings** tab to select the language character and symbol support to be used.

5. Finalize configuration settings by clicking **OK**.

3.4 Step 2: Launch events processing

You are now required to define the event sources i.e. the computers from which events will be collected.


Quick Start Dialog
Welcome to GFI EventsManager
Select the first action you want to perform
Process events - local computer
Use this option to quick start the processing of windows events present on this computer.
Process events - selected machines
Use this option to quick start the processing of windows events present on specific event souces (e.g. computers, etc.)
Customize...
Use this option to customize GFI EventsManager customization settings(e.g. enable Syslog and Snmp trap processing, key event notifications, etc.)
Help me choose ...

Screenshot 8 - Quick Start Dialog

From the Quick Start dialog three different types options can be selected:

1. **Process events - local computer:** This option defines the local computer as the events source machine. This option is highly recommended for first time users who want to gather events on the machine where GFI EventsManager is installed.

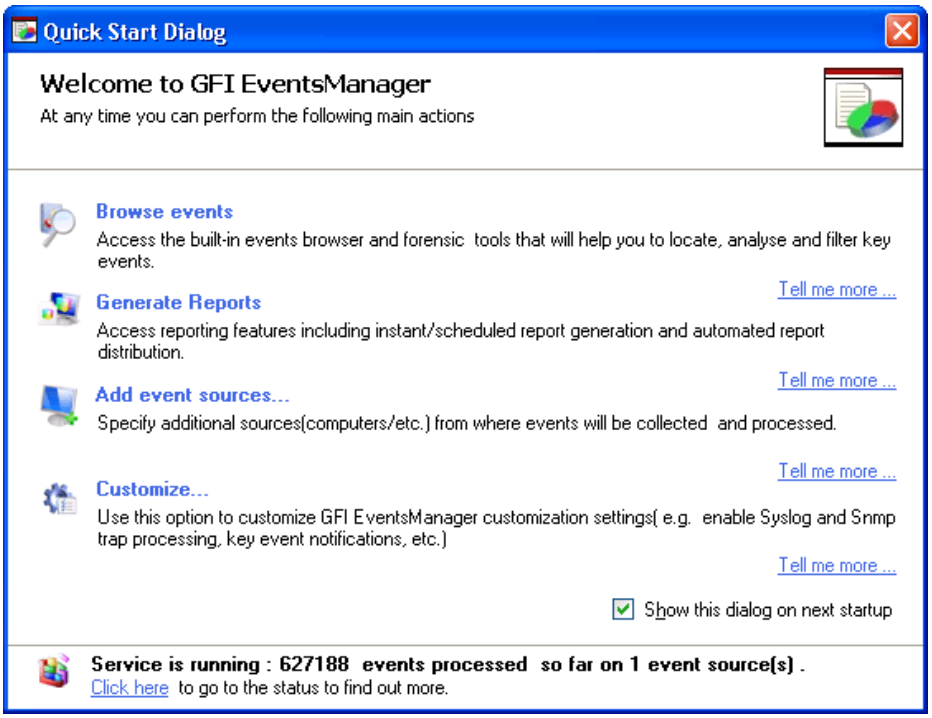
2. **Process events - selected machines:** This option defines a specific range of networked machines as the events sources. This option is recommended for first time users who want to gather information on a wide range of networked computers.

3. **Customize:** This advanced option enables you to customize different types of events or different types of sources (e.g. Syslog and SNMP Trap processing) and is recommended for advanced users.

3.4.1 Processing events from the local computer

To process event logs from the local machine:

1. From the Quick Start Dialog, click **Process events - local computer.** GFI EventsManager will start to collect events from the local machine immediately.

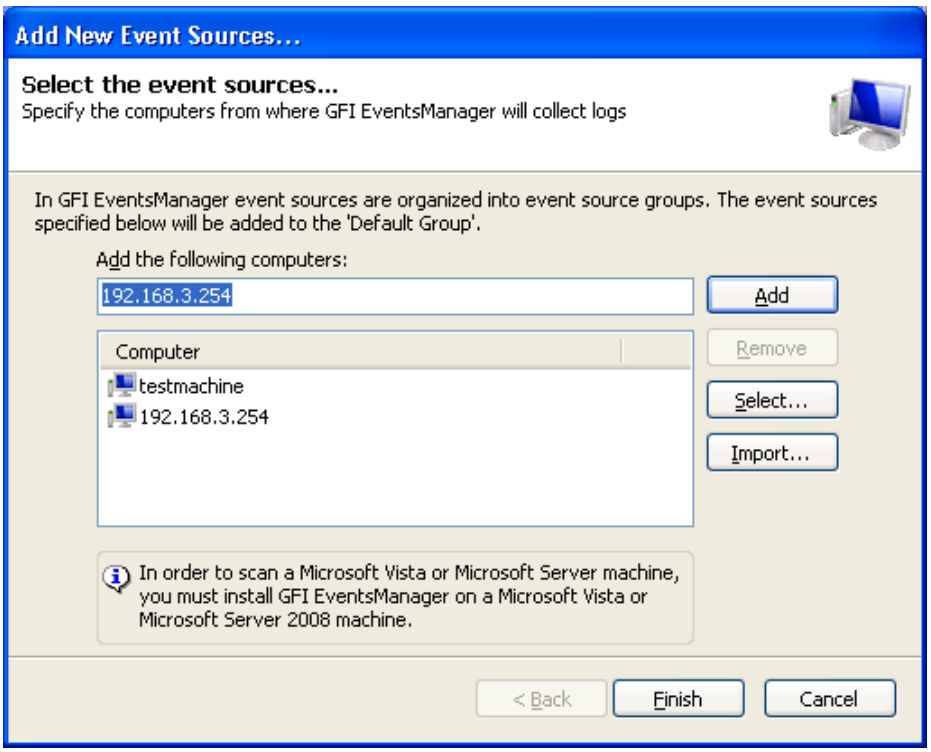

Quick Start Dialog
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyse and filter key events.
Tell me more ...
Generate Reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more ...
Add event sources...
Specify additional sources(computers/etc.) from where events will be collected and processed.
Tell me more ...
Customize...
Use this option to customize GFI EventsManager customization settings(e.g. enable Syslog and Snmp trap processing, key event notifications, etc.)
Tell me more ...
Show this dialog on next startup
Service is running : 627188 events processed so far on 1 event source(s) .
Click here to go to the status to find out more.

Screenshot 9 - Events processed from local machine

On completion, the number of events that have been processed is displayed in the information bar as illustrated in the screenshot above.

Refer to 'Analyzing events and generating reports' section in this manual to learn more about the next steps.

3.4.2 Processing events from selected machines


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the 'Default Group'.
Add the following computers:
192.168.3.254
Add
Remove
Computer
testmachine
192.168.3.254
Select...
Import...
In order to scan a Microsoft Vista or Microsoft Server machine, you must install GFI EventsManager on a Microsoft Vista or Microsoft Server 2008 machine.
< Back
Finish
Cancel

Screenshot 10 - Process events from selected machines

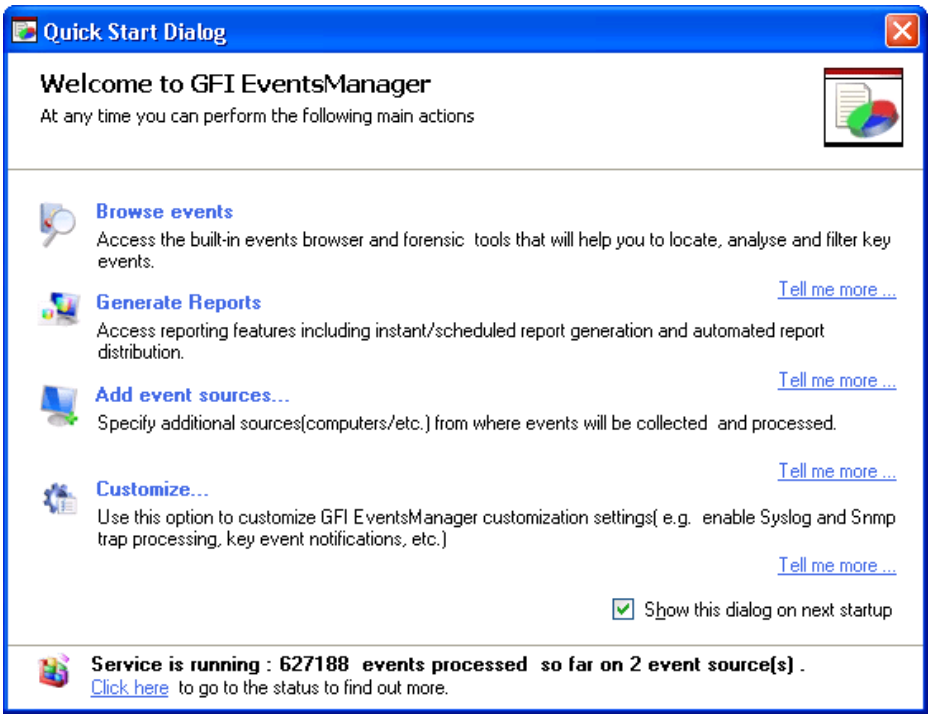
To collect event logs from selected machines:

1. From the Quick Start Dialog, click **Process events - selected machines.** This will bring up the 'Add New Event Sources' wizard.

2. Specify the name/IP of the new event source and click **Add**. Repeat until you have specified all the event sources to add to this group.

NOTE: To import the list of event sources from a text file click **Import** button. To select event sources from a list, click **Select** button.

3. Click **Finish** to finalize settings. GFI EventsManager will collect events from the configured sources immediately after clicking **Finish**.


Quick Start Dialog
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyse and filter key events.
Tell me more ...
Generate Reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more ...
Add event sources...
Specify additional sources(computers/etc.) from where events will be collected and processed.
Tell me more ...
Customize...
Use this option to customize GFI EventsManager customization settings(e.g. enable Syslog and Snmp trap processing, key event notifications, etc.)
Tell me more ...
Show this dialog on next startup
Service is running : 627188 events processed so far on 2 event source(s) .
Click here to go to the status to find out more.

Screenshot 11 - Events processed from selected machines

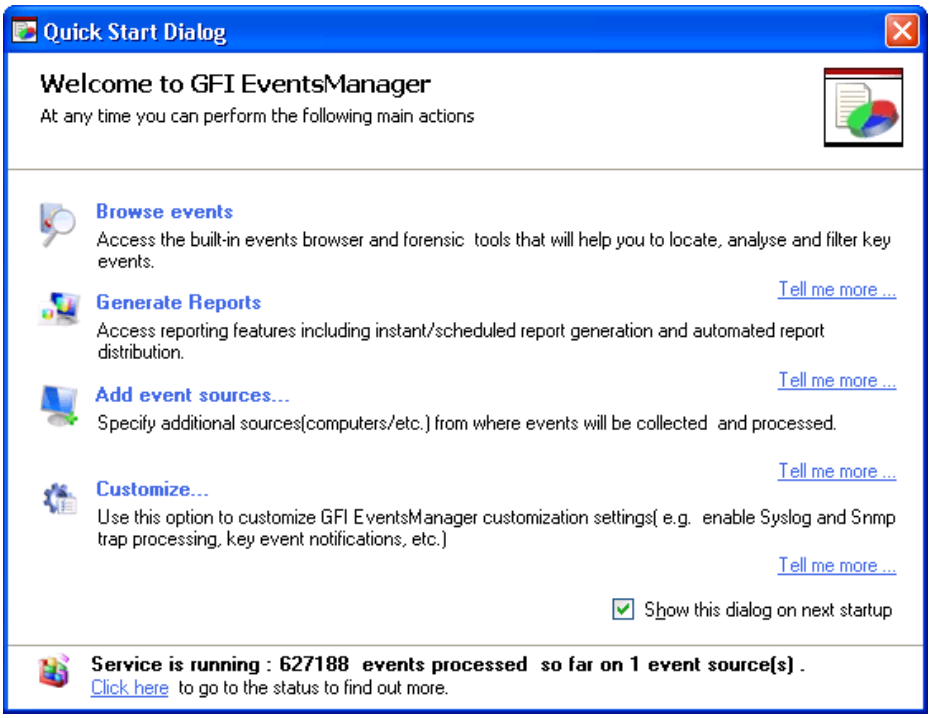
On completion, the number of events processed is displayed in the bottom bar as illustrated in the screenshot above.

Refer to the 'Analyze events and generate reports' section in this manual to learn more about the next steps.

3.5 Step 3: Analyze events and generate reports

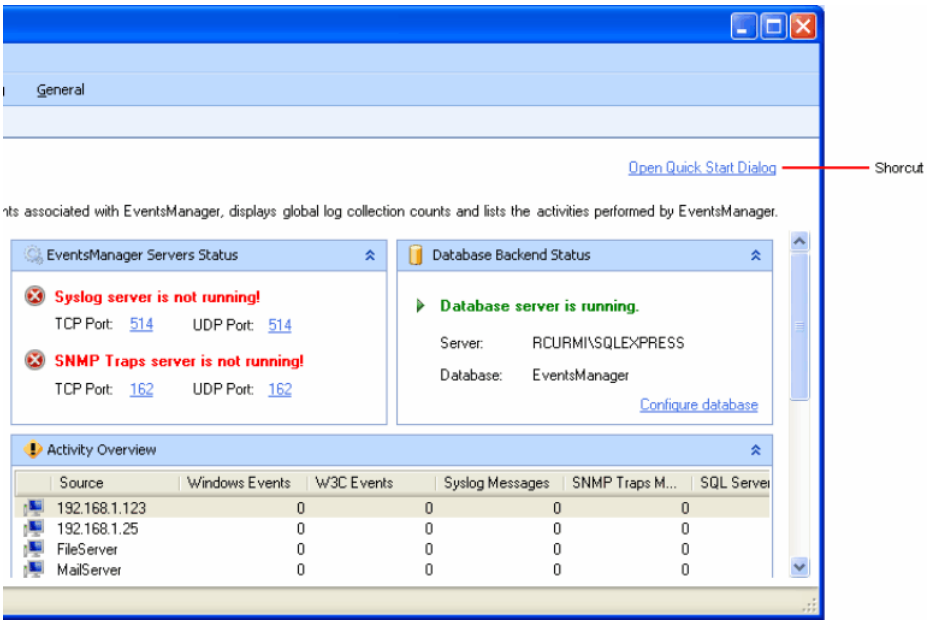
3.5.1 Navigating the Quick Launch Console

You can now analyze the event information collected and generate reports based on the data gathered


Quick Start Dialog
Welcome to GFI EventsManager
At any time you can perform the following main actions
Browse events
Access the built-in events browser and forensic tools that will help you to locate, analyse and filter key events.
Tell me more ...
Generate Reports
Access reporting features including instant/scheduled report generation and automated report distribution.
Tell me more ...
Add event sources...
Specify additional sources(computers/etc.) from where events will be collected and processed.
Tell me more ...
Customize...
Use this option to customize GFI EventsManager customization settings(e.g. enable Syslog and Snmp trap processing, key event notifications, etc.)
Tell me more ...
Show this dialog on next startup
Service is running : 627188 events processed so far on 1 event source(s) .
Click here to go to the status to find out more.

Screenshot 12 - GFI EventsManager Quick Launch Console

The Quick Launch Console provides the common next steps that should be undertaken after processing events..



Screenshot 13 - Quick Launch Console shortcut

Closing the Quick Launch Console minimizes it to the user interface. To restore the Quick Launch console, click on the **Open Quick Launch Console** link Open Quick Start Dialog from the top right-hand corner of the GFI EventsManager user interface.

Browse events

Access the built-in events and forensic tools that will help you to locate,

analyze and filter key events. Clicking **Browse events,** opens the **Windows Events Browser** window in the **Events Browser**. For more information refer to the 'Event browsing' chapter in this manual.

Generate reports

Access reporting features including instant/scheduled report generations and automated report distribution. Clicking **Generate Reports,** opens the **Reporting** tab. For more information refer to the 'Generating reports' chapter in this manual.

Add event sources

Specify additional sources from where events are collected and processed. Clicking **Add event sources,** opens the 'Add New Event Sources' dialog.

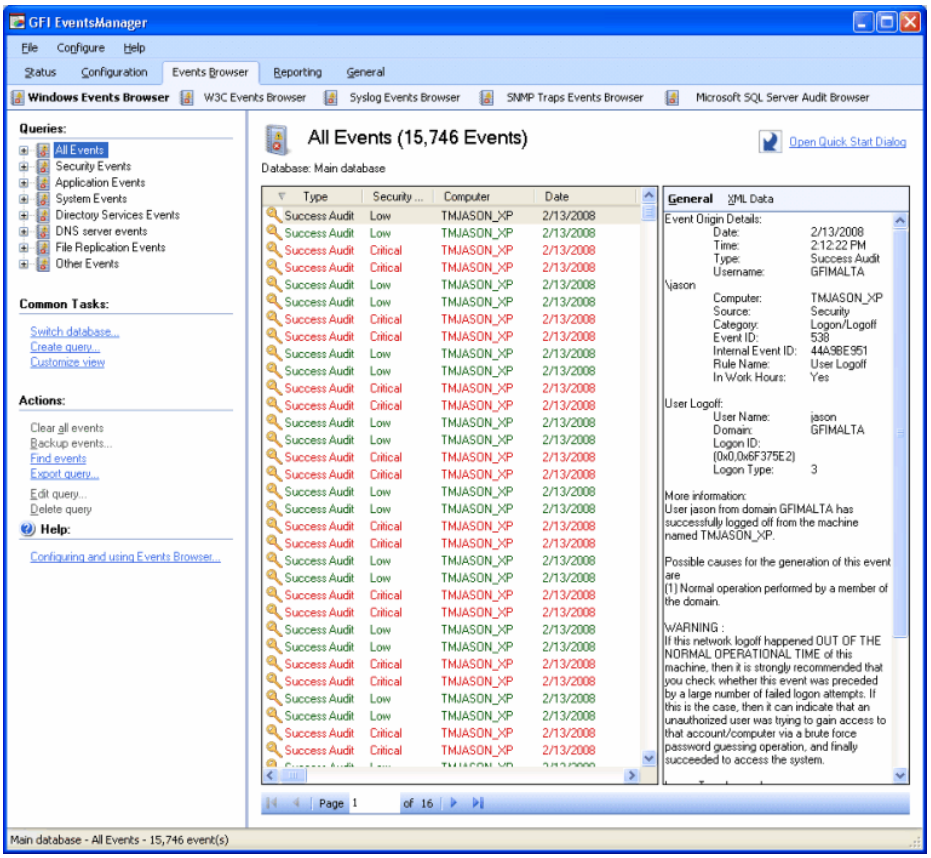
Customize

Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, key events notifications, etc. Clicking on **Customize** opens the Quick Start Dialog: Customization Options dialog. For more information refer to the 'Processing custom events' section in this manual.

4 Event browsing

4.1 Introduction

The Event Browsing option allows you to access and browse processed or unprocessed events/logs that are currently stored in the main or backup database backbends.


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Windows Events Browser W3C Events Browser Syslog Events Browser SNMP Traps Events Browser Microsoft SQL Server Audit Browser
Queries:
All Events
Security Events
Application Events
System Events
Directory Services Events
DNS server events
File Replication Events
Other Events
Common Tasks:
Switch database...
Create query...
Customize view
Actions:
Clear all events
Backup events...
Find events
Export query...
Edit query...
Delete query
Help:
Configuring and using Events Browser...
All Events (15,746 Events)
Open Quick Start Dialog
Database: Main database
Type Security ... Computer Date
Success Audit Low TMJASON_XP 2/13/2008
Success Audit Critical TMJASON_XP 2/13/2008
General XML Data
Event Origin Details:
Date: 2/13/2008
Time: 2:12:22 PM
Type: Success Audit
Username: GFIMALTA
\jason
Computer: TMJASON_XP
Source: Security
Category: Logon/Logoff
Event ID: 538
Internal Event ID: 44A9BE951
Rule Name: User Logoff
In Work Hours: Yes
User Logoff:
User Name: jason
Domain: GFIMALTA
Logon ID: (0x0,0x6F375E2)
Logon Type: 3
More information:
User jason from domain GFIMALTA has successfully logged off from the machine named TMJASON_XP.
Possible causes for the generation of this event are
(1) Normal operation performed by a member of the domain.
WARNING :
If this network logoff happened OUT OF THE NORMAL OPERATIONAL TIME of this machine, then it is strongly recommended that you check whether this event was preceded by a large number of failed logon attempts. If this is the case, then it can indicate that an unauthorized user was trying to gain access to that account/computer via a brute force password guessing operation, and finally succeeded to access the system.
Page 1 of 16
Main database - All Events - 15,746 event(s)

Screenshot 14 - GFI EventsManager: Events Browser

Use the Events Browser for forensic analysis of events. All events accessible through the events browser are organized (by log type) in 4 tabs; **Windows Events Browser** tab, **W3C Events Browser** tab **Syslog Events Browser** tab, **SNMP Traps Events Browser** tab and **Microsoft SQL Server audit Browser** tab. This way you can quickly access the events belonging to a particular log type. Event data is organized into columns and clicking on a particular event will show additional information in a dedicated events description pane.

Event ID: 532	
Source	adsctlr
Type	Warning
Description	Failed to connect to the device (device name: <name> IP address: <IP address>): Failed to connect to the remote computer because of certificate issues. Also check the date on the target computer.
Comments	Ionut Marin (Last update 10/2/2005): Microsoft has a hotfix that might solve this problem. See M875533 for details. Bryan Fowler (Last update 10/1/2005): In my case the BIOS date was incorrect. I corrected it and then I was able to connect to the deployment agent successfully.
Links	M875533
Search	Microsoft Support - Microsoft Search - Google Groups - Google Microsoft - EventID.Net Queue - More links...
Various	Send comments - Notify me when updated

Screenshot 15 - Event details provided on the web-page

Windows events, descriptions are organized in two tabs accessible from the events description field:

- **General tab -** Contains events information in the legacy format that was standard for pre-Microsoft Windows Vista event logs.
- **XML Data tab -** Contains events information in the new XML based Microsoft Windows Vista format.

Use the link provided in the event description pane to access:

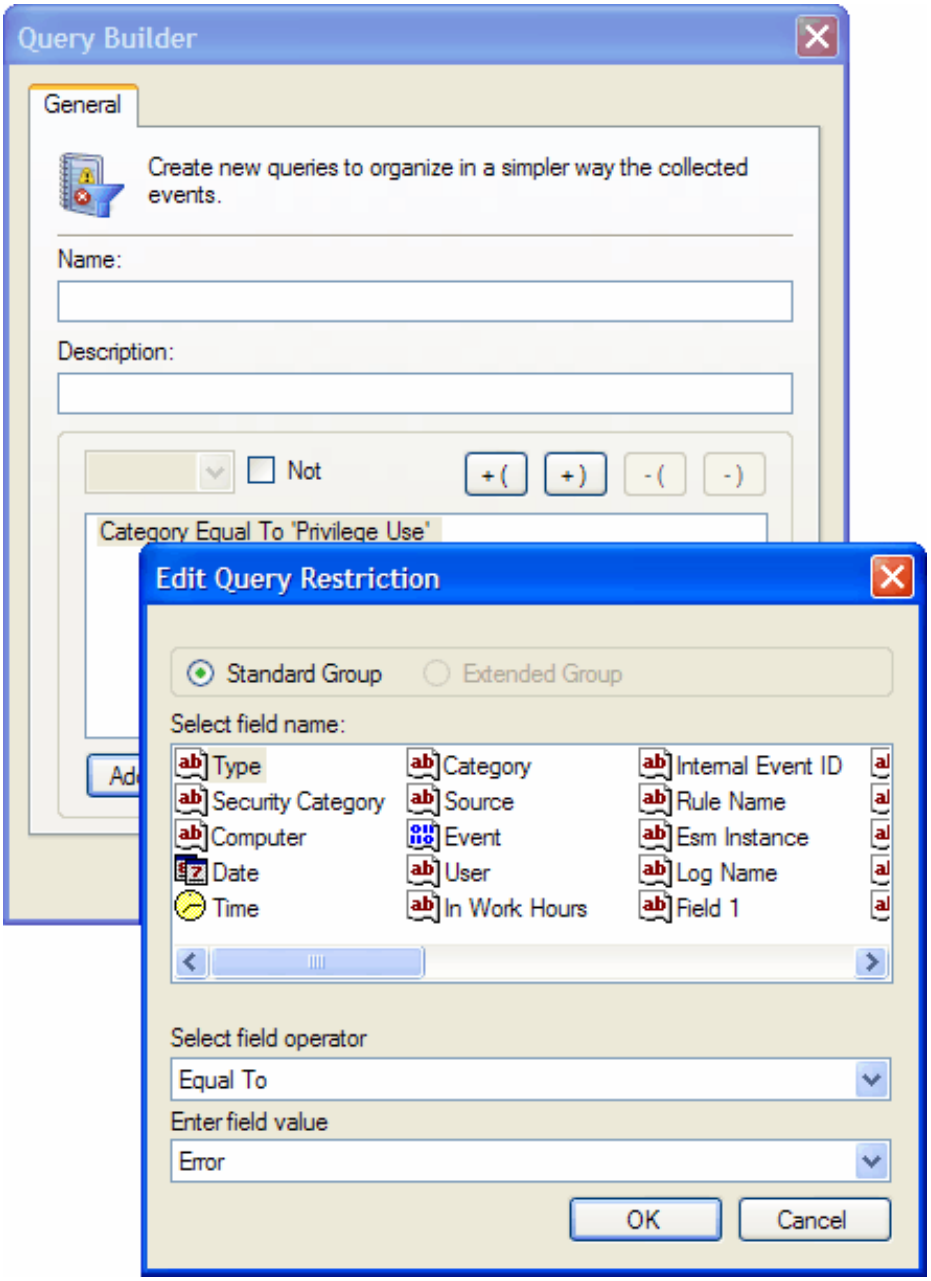
- A more detailed description of the event
- Information and links that explain what causes this type of event
- Hints and tips on how to possibly solve any existing issues.

Event browsing tools

Event analysis is quite a demanding task; GFI EventsManager is equipped with specialized tools that simplify the search for specific events as well as enable the export of events to CSV files. These specialized tools include:

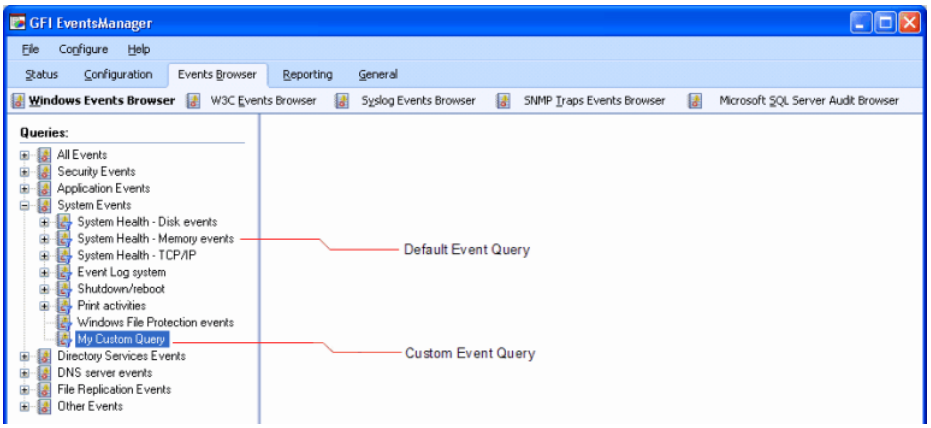
- An event filter/query builder
- Event color-coding options
- Event finder tool
- Export events tool.

Event filter/query builder



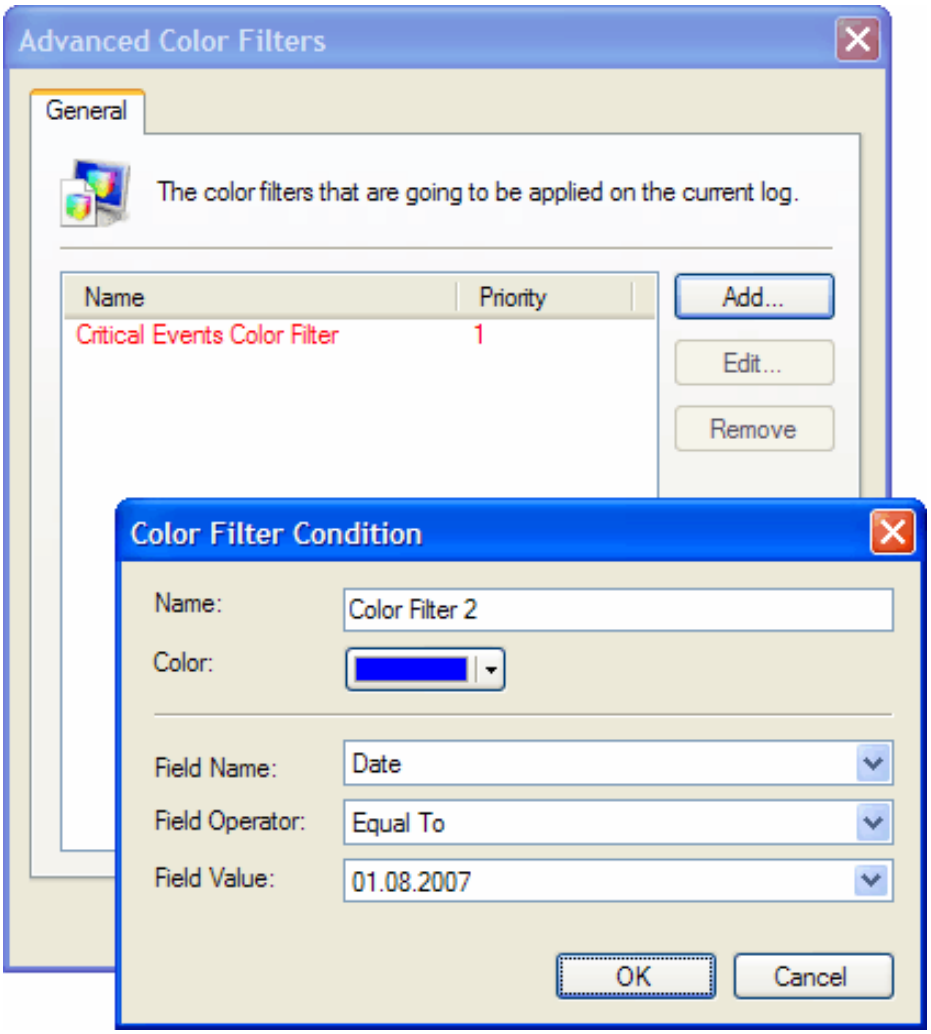
Screenshot 16 - Custom query builder

Use the event query builder that ships with GFI EventsManager to create custom filters that sift events data and display only the information that you need to browse - without deleting one single record from your database backend. Further to this GFI EventsManager ships with pre-configured queries that can filter events without any configuration effort - just click and go.



Screenshot 17 - Default and custom event queries

Event color-coding options



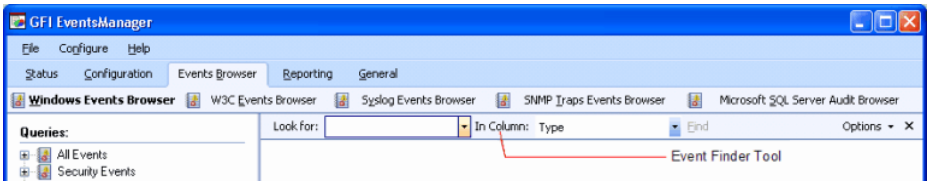
Screenshot 18 - Event color coding filters

Use the event color-coding tool to tint key events in a particular color. This way the required events are easier to locate during event browsing. For example, you can create a query that shows events classified as Critical or High and at the same time color in red all Critical events having event ID 231.

The configuration of color-codes is carried out through a dedicated query builder. Use this query builder to specify:

- The conditions that define which events must be colored
- The colors to be used when showing these events.

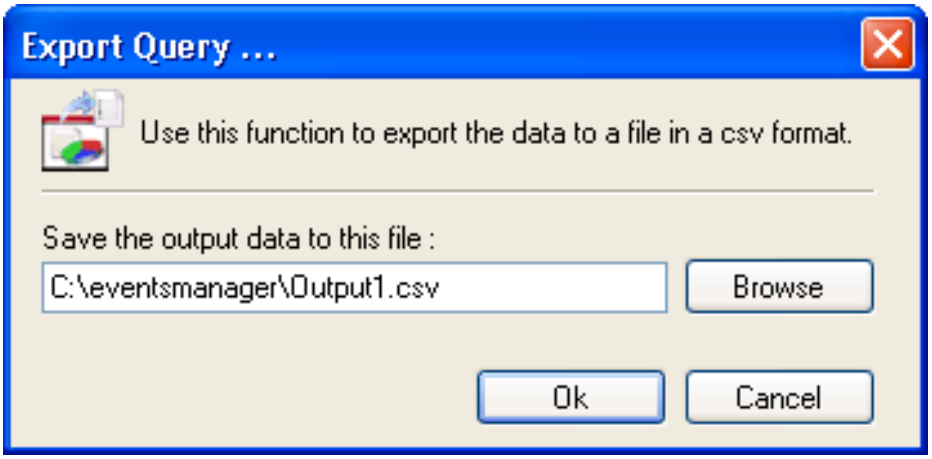
Event finder tool



Screenshot 19 - Event finder tool

Use the event finder tool to locate events that match a specific search string. For example, you can search events that have a specific ID or which contain specific keywords in the description.

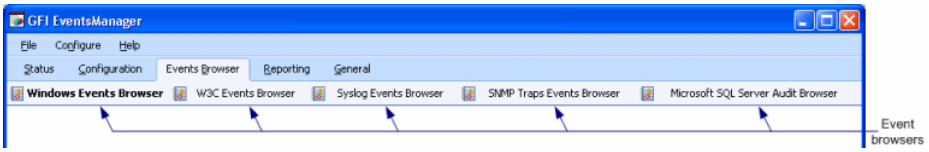
Export events tool


Export Query ...
Use this function to export the data to a file in a csv format.
Save the output data to this file :
C:\eventsmanager\Output1.csv
Browse
Ok
Cancel

Screenshot 20 - Export events tool

Use the export events tool to save events data to CSV file . For more information refer to the 'Export events tool' section in this manual.

4.2 Accessing and browsing stored event logs


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Windows Events Browser W3C Events Browser Syslog Events Browser SNMP Traps Events Browser Microsoft SQL Server Audit Browser
Event browsers

Screenshot 21 - Events browsers

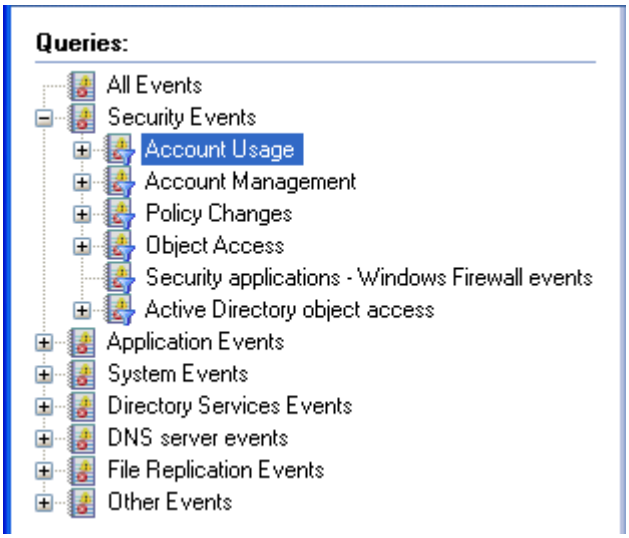
To access and browse events stored in the database backend click on the **Events Browser** tab and select a browser accordingly.

4.3 Applying event queries

To filter event during browsing:

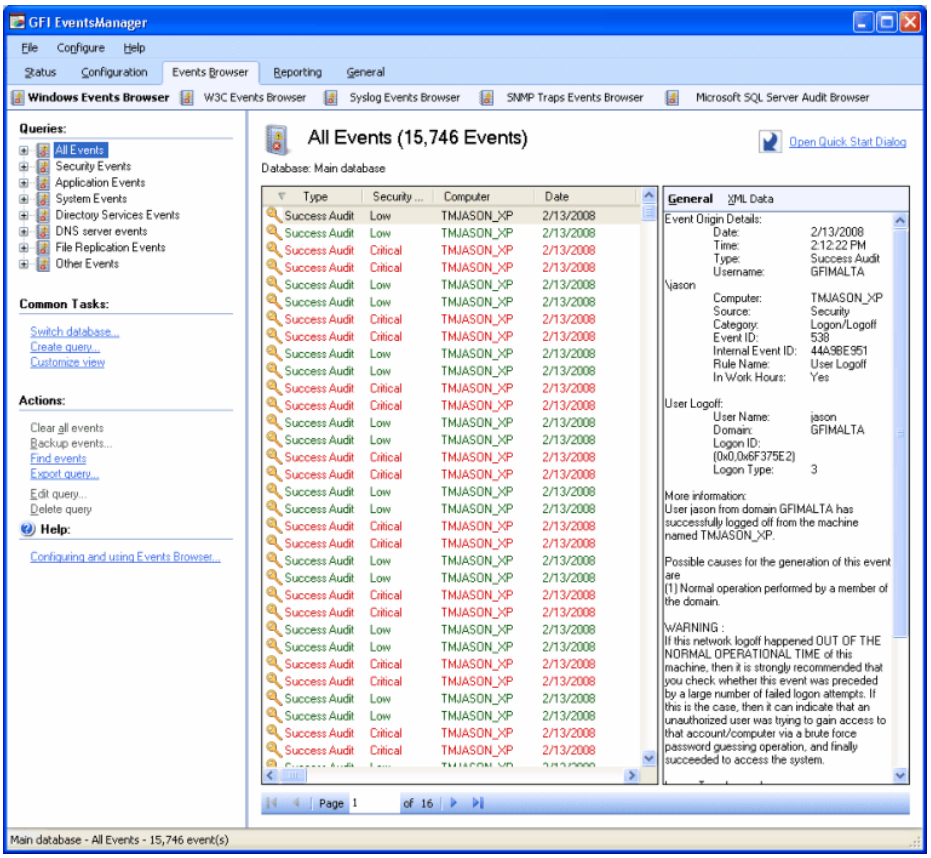
1. Click on the **Events Browser** tab and select the events browser required.

2. From the left pane select the required events filter (such as the Accounts Usage filter). Results will be displayed in the browser (right pane).



Screenshot 22 - Selecting a filter

4.4 Creating custom event queries

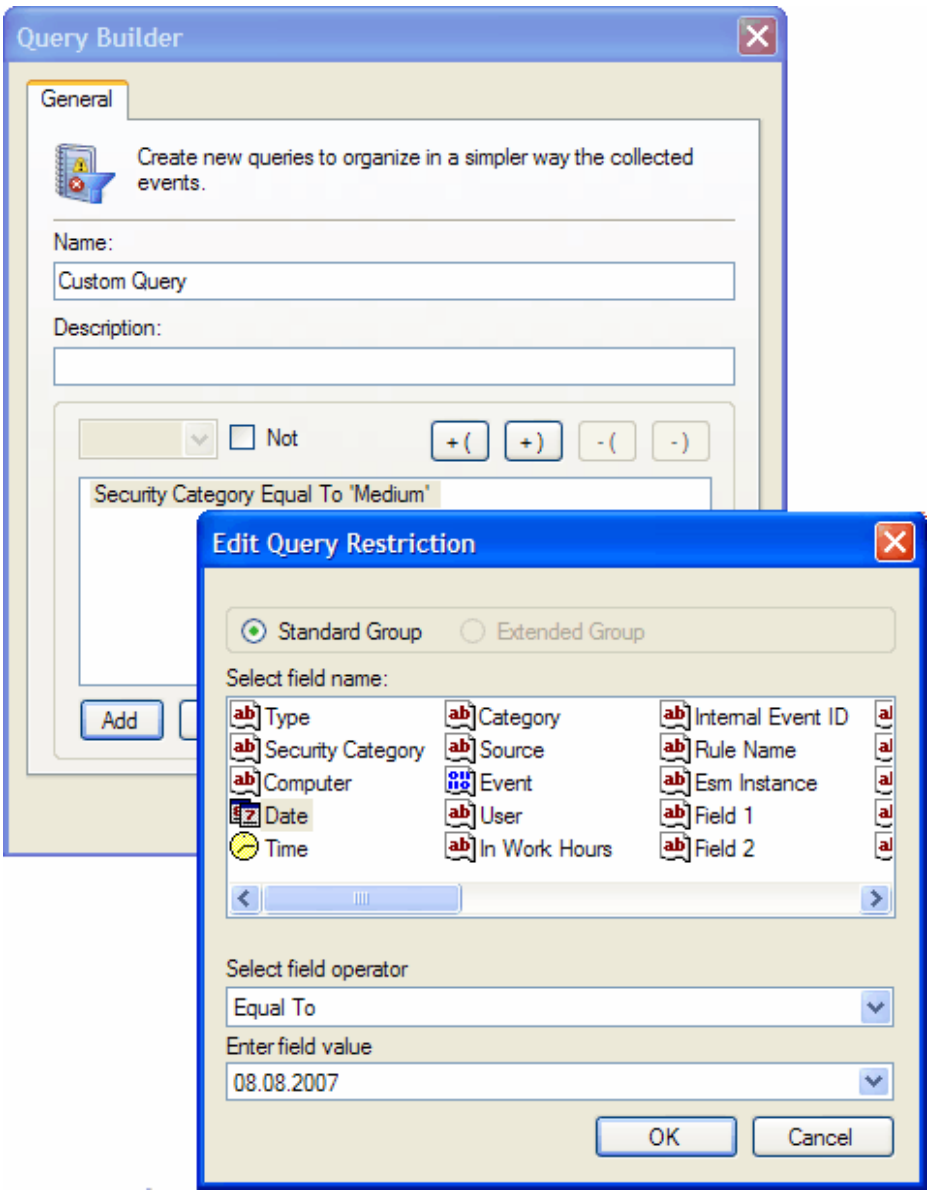


Screenshot 23 - GFI EventsManager: Events Browser

In GFI EventsManager, custom queries are added as a sub-node within the default queries that ship with the product. To create custom event queries:

1. Click on the **Events Browser** tab and select an events browser accordingly.

2. Right-click on the default query where the new event query will be created and select **Create query…** This will bring up the event query builder.



Screenshot 24- Custom query builder

3. Specify a name and a description for the new query.

4. Click **Add**, configure the required query condition(s) and click **OK**. Repeat until all required query conditions have been specified.

5. Click **OK** to finalize your settings.

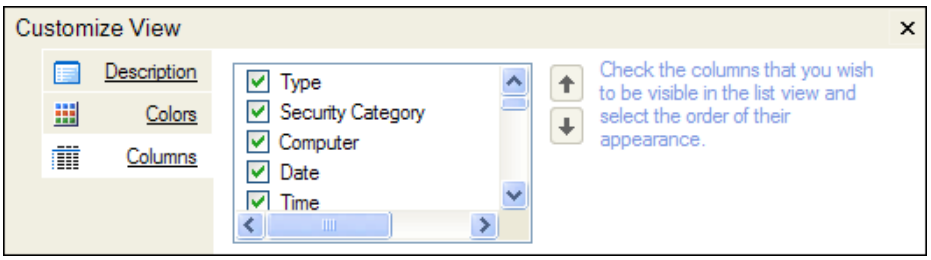
4.5 Customizing the event viewer pane

Selecting columns to be displayed

To select which columns will be displayed in the Log Browser's viewing pane:

1. Click on the **Events Browser** tab and select an events browser accordingly.

2. Select the **Customize view** option from the 'Common Tasks' area in the left pane.



Screenshot 25 - Customize view: columns

3. Select the **Columns** option.

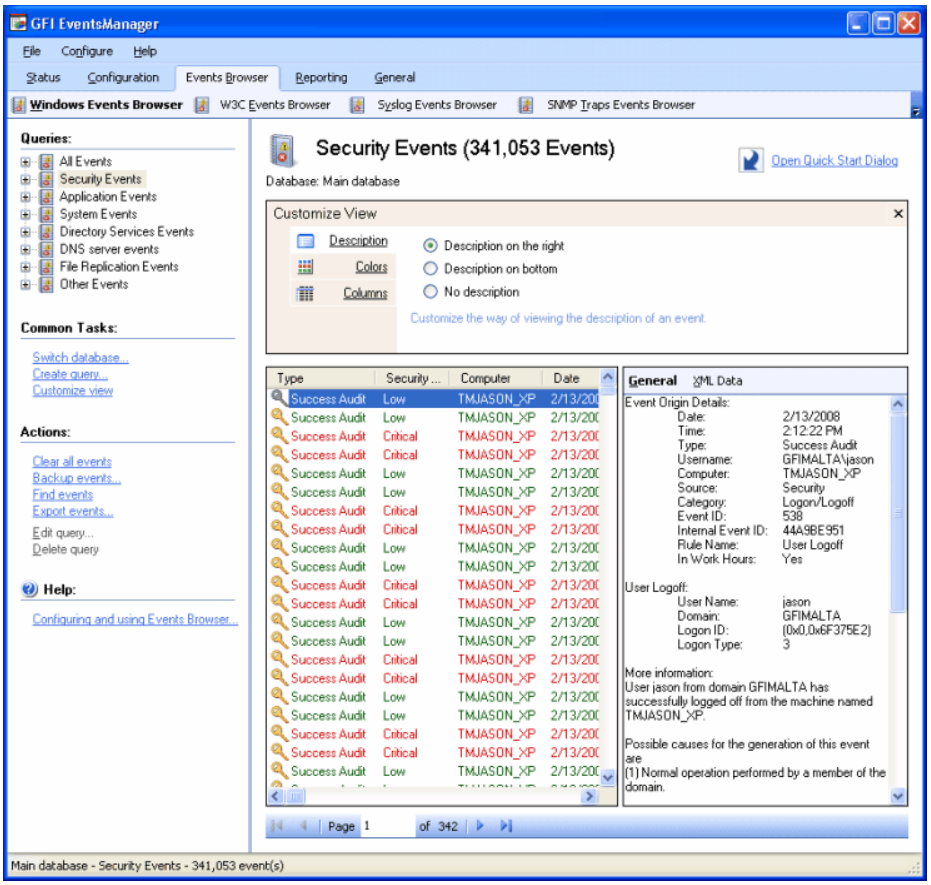
4. Select the columns that will be displayed in the viewing pane. Use the up/down arrows on the side to define the order in which the columns will be shown.

5. Close the customize view pane to finalize your settings.

Customize the position of the description window

GFI EventsManager allows you to customize the right viewing pane. To achieve this:

1. Click on the **Events Browser** tab and select an events browser accordingly.



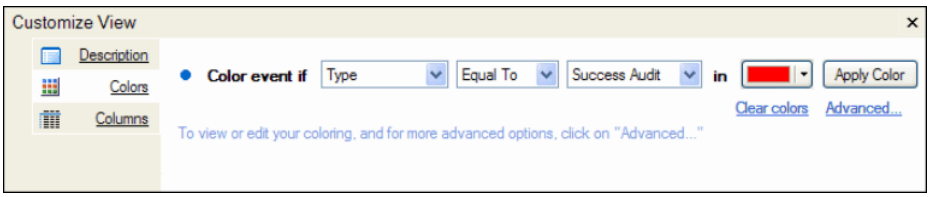
Screenshot 26 - Customize view

2. Click the **Customize view** option from the 'Common Tasks' pane.

3, Customize the browser view accordingly.

4.6 Configuring event color coding

Assigning a color-code to a specific event



Screenshot 27 - Assigning event color-codes

To assign a color code to a specific event:

1. Click on the **Events Browser** tab and select an events browser accordingly.

2. Select the **Customize view** option and from the right pane, select the **Colors** option.

3... Specify event filter parameters including the color to be applied to the sifted events.

4. Click on the **Apply Color** button to finalize your settings.

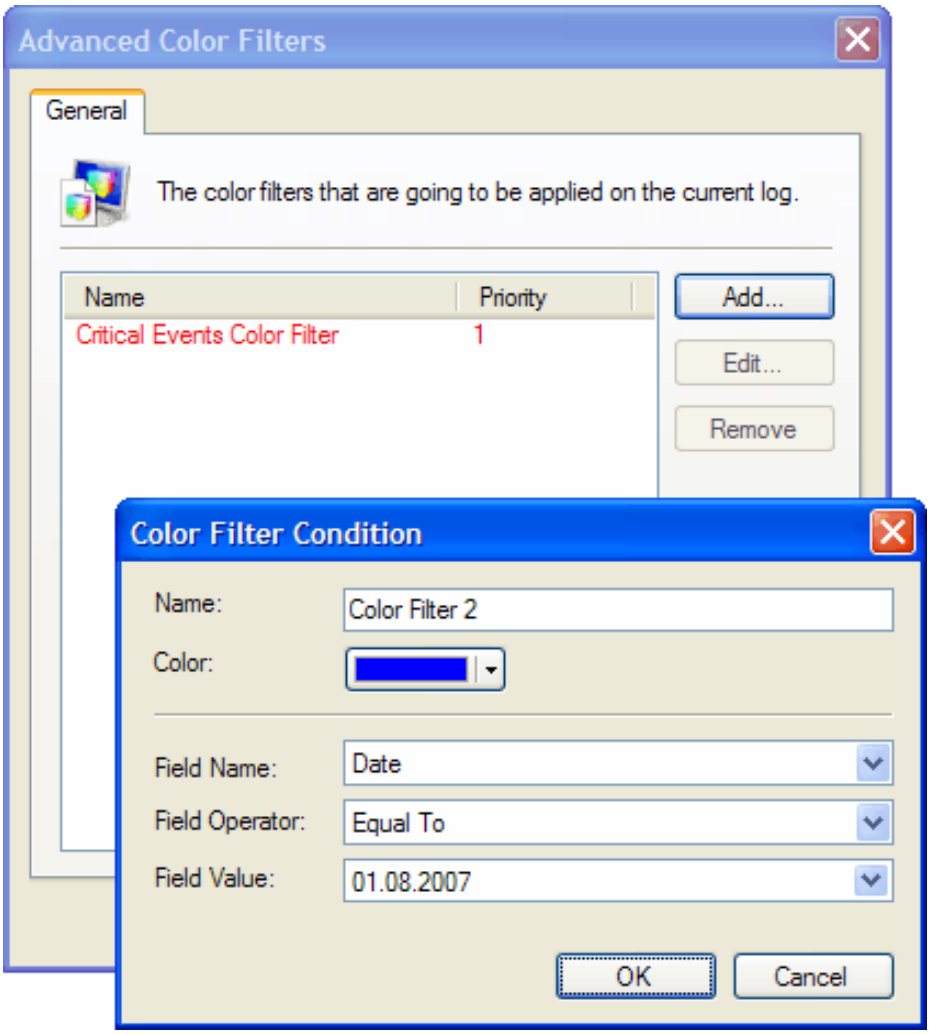
NOTE: Use the **Clear color filters** option to clear all color settings.

Assigning different color-codes to multiple events

To assign different color-codes to multiple events:

1. Click on the **Events Browser** tab and select an events browser accordingly.

2. Select the **Customize view** option. From the right pane, select the **Colors** option and click **Advanced**.



Screenshot 28 - Advanced Color Filter

3. Click on the **Add** button. Specify filter name and configure event filter parameters.

4. Click on the **OK** button to save filter settings.

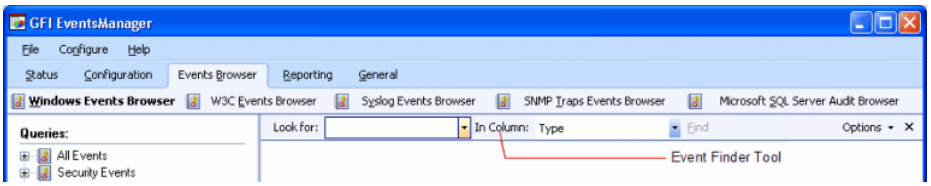
5. Repeat until all required event filter conditions have been configured. Click **OK** to finalize your settings.

4.7 Event finder tool

Use the event finder tool to search and locate specific events using simple customizable filters. To search for a particular event:

1. Click on the **Events Browser** tab and select an events browser accordingly

2. From the left pane, select the **Find events** option.



Screenshot 29 - Event finder tool

3. Configure the event search parameters through the options provided on top of the right pane. To trigger a case sensitive search, click on **Options** and select the **Match case** option.

4. Click on the **Find** button to trigger the search.

4.8 Export events tool

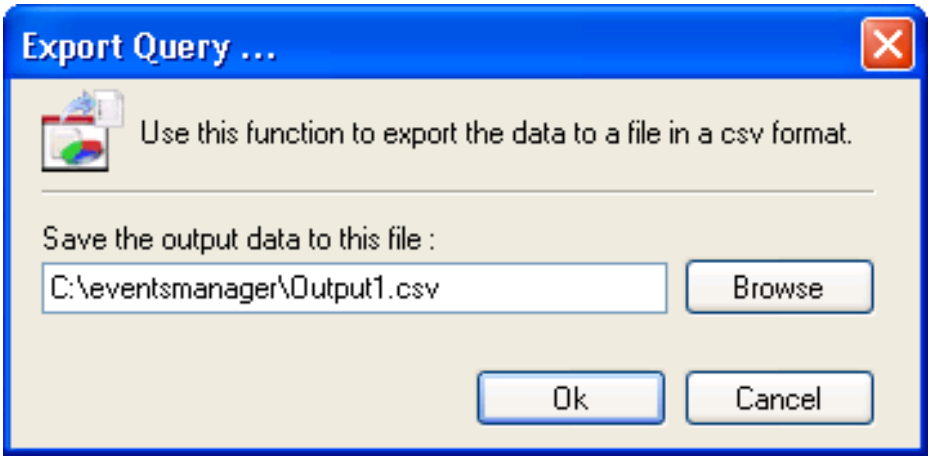
GFI EventsManager allows you to export events data to CSV files directly from the built-in event-browsers. This is extremely convenient especially when further processing of events data is required including:

- Distribution of key events data via email
- Running automated scripts which convert CSV exported events data to HTML for upload on web/company intranet
- Generation of graphical management reports and statistical data using native tools like Microsoft Excel
- Generation of custom reports using third party applications.
- Interfacing events data with applications and scripts built in-house

To export events to CSV:

1. Click **Events Browser** tab and select the required event browser accordingly.

2. Select the events to be exported. Right-click on the selection and choose **Export events…** .


Export Query ...
Use this function to export the data to a file in a csv format.
Save the output data to this file :
C:\eventsmanager\Output1.csv
Browse
Ok
Cancel

Screenshot 30 - Export events tool

3. Specify the location where exported events will be saved and click **OK** to trigger the export operation.

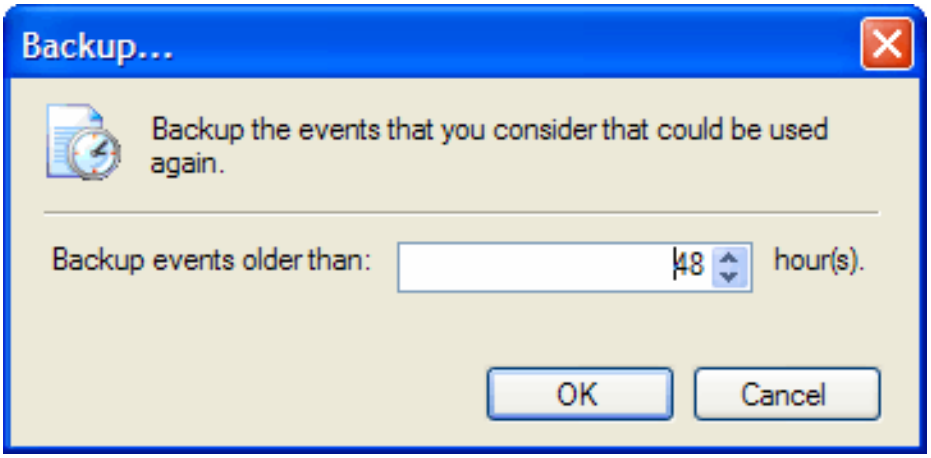
4.9 Backup events

GFI EventsManager allows you to backup the events stored in the main database backend. This way you can reduce the size of your main database backend but at the same time keep all your event records for historical and forensic investigation purposes.

Use the backup events feature to backup events that are older than a specific amount of hours. For example, you can choose to backup events that are older than 48 hours. To backup events:

1. Click on the **Events Browser** tab and select an events browser accordingly.

2. From the left pane, select the **Backup events** option.



Screenshot 31 - Backup events dialog box

3. Specify backup parameters and click on the **OK** button to finalize your settings.

4.10 Switching databases

For event browsing purposes, GFI EventsManager allows you to switch between the main and backup database backend. Use this feature to browse events that have been backed up, using the tools provided in the Events Browser. To achieve this:

1. Click on the **Events Browser** tab and select an events browser accordingly.

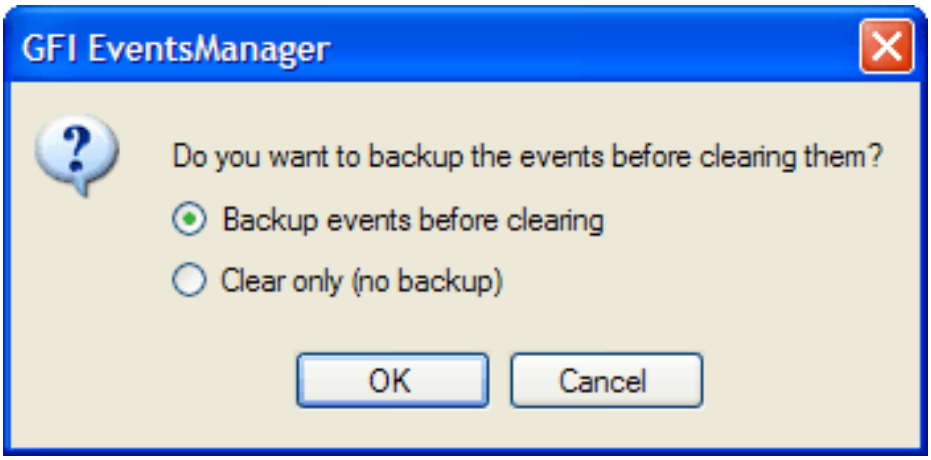
2. From the left pane select the **Switch to main/backup database** option.

4.11 Clear all events

To clear ALL the events stored in the currently selected database:

1. Click on the **Events Browser** tab and select an events browser accordingly.

2. From the left pane select the **Clear all events** option.



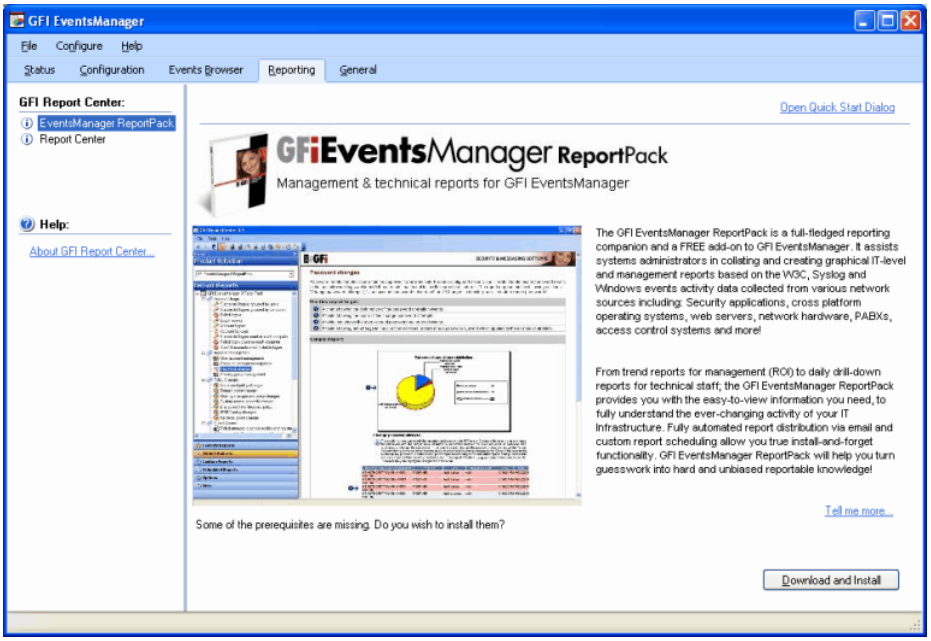
Screenshot 32 - Clear all events dialog box

3. If you are currently browsing events from the main database, specify whether you want to backup events before clearing.

5 Generating reports

5.1 Introduction

GFI EventsManager provides you with a free, fully-fledged reporting companion to GFI EventsManager - GFI EventsManager ReportPack. It enables you to generate graphical IT-level, technical and management reports based on the hardware and software events processed by GFI EventsManager. Hardware and software event sources include any networked component that generate Syslog messages or record/log events to Windows and/or W3C event logs. These include computers, network devices, PABXs, and third party software solutions.


GFI EventsManager
File
Configure
Help
Status
Configuration
Events Browser
Reporting
General
GFI Report Center:
EventsManager ReportPack
Report Center
Help:
About GFI Report Center...
Open Quick Start Dialog
GFiEventsManager ReportPack
Management & technical reports for GFI EventsManager
The GFI EventsManager ReportPack is a full-fledged reporting companion and a FREE add-on to GFI EventsManager. It assists systems administrators in collating and creating graphical IT-level and management reports based on the W3C, Syslog and Windows events activity data collected from various network sources including: Security applications, cross platform operating systems, web servers, network hardware, PABXs, access control systems and more!
From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI EventsManager ReportPack provides you with the easy-to-view information you need, to fully understand the ever-changing activity of your IT infrastructure. Fully automated report distribution via email and custom report scheduling allow you true install-and-forget functionality. GFI EventsManager ReportPack will help you turn guesswork into hard and unbiased reportable knowledge!
Tell me more...
Some of the prerequisites are missing. Do you wish to install them?
Download and Install

Screenshot 33 - Reporting

To access GFI EventsManager ReportPack, click the **Reporting** tab.

NOTE: To generate reports, the following add-ins must be downloaded and installed:

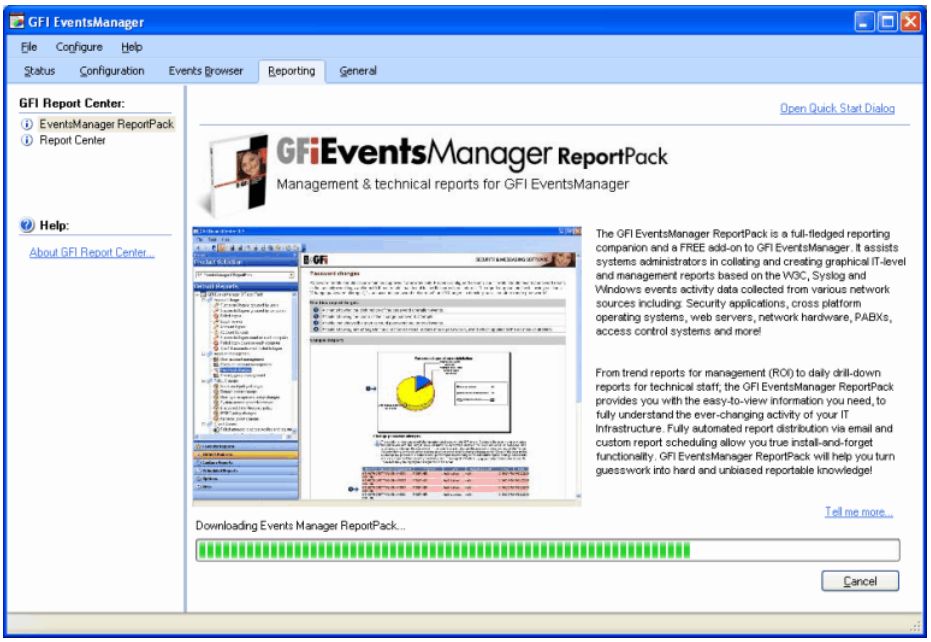
1. GFI ReportCenter framework
2. GFI EventsManager ReportPack

More information on how to download the GFI EventsManager ReportPack and the GFI ReportCenter framework is provided in the 'Download the GFI EventsManager ReportPack' section below.

5.2 Download the GFI EventsManager ReportPack

From the GFI EventsManager Reporting tab, click on **Download and install** button to download and install the GFI EventsManager

ReportPack on the local machine. Prior to installing the GFI EventsManager ReportPack, GFI EventsManager will also prompt you to install any pre-requisites that are required. This includes the GFI ReportCenter framework.

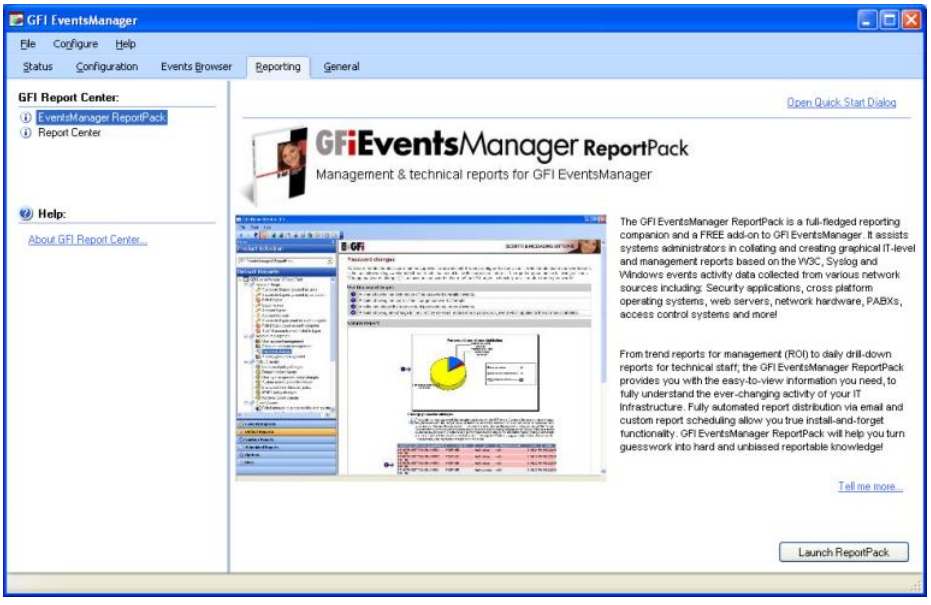

GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
GFI Report Center:
EventsManager ReportPack
Report Center
Help:
About GFI Report Center...
Open Quick Start Dialog
GFiEventsManager ReportPack
Management & technical reports for GFI EventsManager
The GFI EventsManager ReportPack is a full-fledged reporting companion and a FREE add-on to GFI EventsManager. It assists systems administrators in collating and creating graphical IT-level and management reports based on the W3C, Syslog and Windows events activity data collected from various network sources including: Security applications, cross platform operating systems, web servers, network hardware, PABXs, access control systems and more!
From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI EventsManager ReportPack provides you with the easy-to-view information you need, to fully understand the ever-changing activity of your IT infrastructure. Fully automated report distribution via email and custom report scheduling allow you true install-and-forget functionality. GFI EventsManager ReportPack will help you turn guesswork into hard and unbiased reportable knowledge!
Tell me more...
Downloading Events Manager ReportPack...
Cancel

Screenshot 34 - Downloading the GFI EventsManager ReportPack

For installation instructions and more information about the GFI EventsManager ReportPack refer to the GFI EventsManager ReportPack user manual available at:

http://www.gfi.com/eventsmanager/esm8rpmanual.pdf.

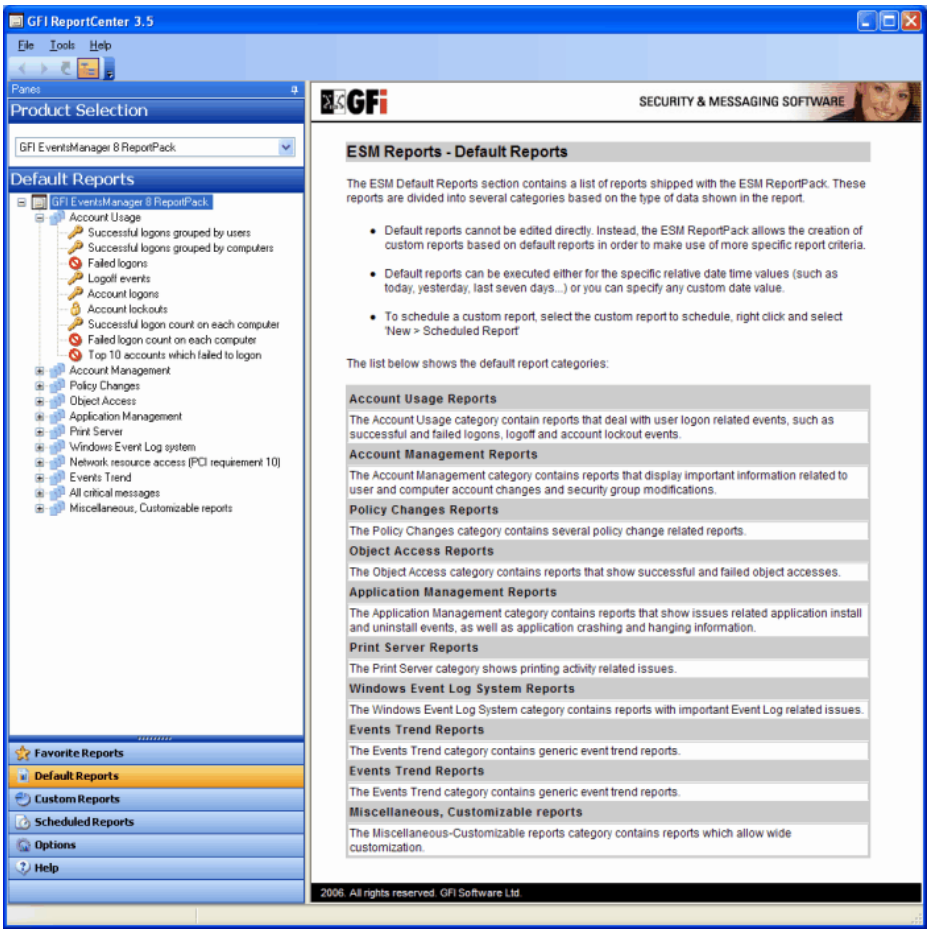
5.3 Launching the GFI EventsManager ReportPack


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
GFI Report Center:
EventsManager ReportPack
Report Center
Help:
About GFI Report Center...
Open Quick Start Dialog
GFiEventsManager ReportPack
Management & technical reports for GFI EventsManager
The GFI EventsManager ReportPack is a full-fledged reporting companion and a FREE add-on to GFI EventsManager. It assists systems administrators in collating and creating graphical IT-level and management reports based on the W3C, Syslog and Windows events activity data collected from various network sources including: Security applications, cross platform operating systems, web servers, network hardware, PABXs, access control systems and more!
From trend reports for management (ROI) to daily drill-down reports for technical staff, the GFI EventsManager ReportPack provides you with the easy-to-view information you need, to fully understand the ever-changing activity of your IT infrastructure. Fully automated report distribution via email and custom report scheduling allow you true install-and-forget functionality. GFI EventsManager ReportPack will help you turn guesswork into hard and unbiased reportable knowledge!
Tell me more...
Launch ReportPack

Screenshot 35 - Launching the GFI EventsManager ReportPack

To generate reports:

1. Click on the **Launch ReportPack** button


GFI ReportCenter 3.5
File Tools Help
Panes
Product Selection
GFI EventsManager 8 ReportPack
Default Reports
GFI EventsManager 8 ReportPack
Account Usage
Successful logons grouped by users
Successful logons grouped by computers
Failed logons
Logoff events
Account logons
Account lockouts
Successful logon count on each computer
Failed logon count on each computer
Top 10 accounts which failed to logon
Account Management
Policy Changes
Object Access
Application Management
Print Server
Windows Event Log system
Network resource access (PCI requirement 10)
Events Trend
All critical messages
Miscellaneous, Customizable reports
Favorite Reports
Default Reports
Custom Reports
Scheduled Reports
Options
Help
SECURITY & MESSAGING SOFTWARE
ESM Reports - Default Reports
The ESM Default Reports section contains a list of reports shipped with the ESM ReportPack. These reports are divided into several categories based on the type of data shown in the report.
Default reports cannot be edited directly. Instead, the ESM ReportPack allows the creation of custom reports based on default reports in order to make use of more specific report criteria.
Default reports can be executed either for the specific relative date time values (such as today, yesterday, last seven days...) or you can specify any custom date value.
To schedule a custom report, select the custom report to schedule, right click and select 'New > Scheduled Report'
The list below shows the default report categories:
Account Usage Reports
The Account Usage category contain reports that deal with user logon related events, such as successful and failed logons, logoff and account lockout events.
Account Management Reports
The Account Management category contains reports that display important information related to user and computer account changes and security group modifications.
Policy Changes Reports
The Policy Changes category contains several policy change related reports.
Object Access Reports
The Object Access category contains reports that show successful and failed object accesses.
Application Management Reports
The Application Management category contains reports that show issues related application install and uninstall events, as well as application crashing and hanging information.
Print Server Reports
The Print Server category shows printing activity related issues.
Windows Event Log System Reports
The Windows Event Log System category contains reports with important Event Log related issues.
Events Trend Reports
The Events Trend category contains generic event trend reports.
Events Trend Reports
The Events Trend category contains generic event trend reports.
Miscellaneous, Customizable reports
The Miscellaneous-Customizable reports category contains reports which allow wide customization.
2006. All rights reserved. GFI Software Ltd.

Screenshot 36 - GFI EventsManager ReportPack console

2. The GFI EventsManager ReportPack console will open in a new window. Generate the required reports by right clicking on the desired report.

For more information about the reports and the functionalities of GFI EventsManager ReportPack refer to the GFI EventsManager ReportPack user manual available at:

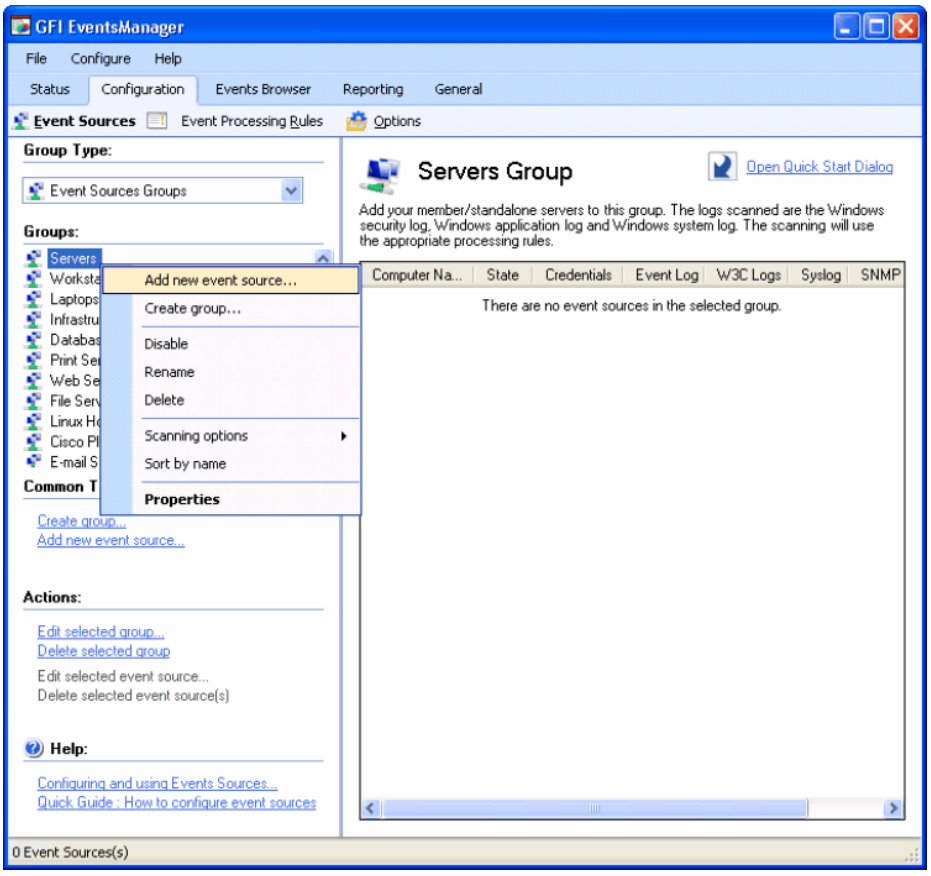
http://www.gfi.com/eventsmanager/esm8rpmanual.pdf.

6 Customizing event sources

6.1 Introduction

Event sources are computers that contain the logs to be processed by GFI EventsManager. In GFI EventsManager, these event sources are organized into specific computer groups. You can create custom event source groups tailored on your network infrastructure or you can use the pre-defined groups that ship by default with this product. GFI EventsManager ships with two distinct event source groups namely 'Event Sources Groups' and 'Database Server Groups'. You can use default groups to distinctively organize and configure the servers, workstations and laptops that will be monitored by GFI EventsManager; or you can choose to group target computers that have specific roles on your network such as web Servers, file servers and data servers.

6.2 Adding new event sources to the computers group



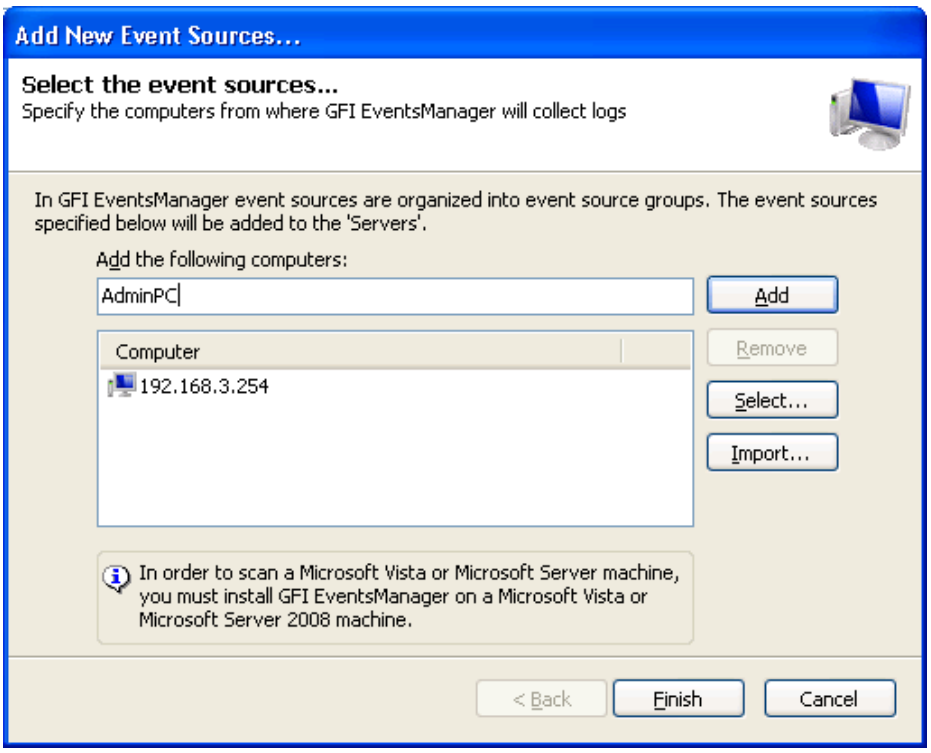
Screenshot 37 - Configuring the computer that will be monitored

To add new event sources to a computer group:

1. Click on the **Configuration** tab and select **Event Sources** from the tab options.

2. From the **Group Type** drop-down, select **Event Sources Groups**.

3. Right-click on the Computer Group which will contain the new event sources and select **Add new event source**. This will bring up the 'Add New Event Sources' dialog.


Add New Event Sources...
Select the event sources...
Specify the computers from where GFI EventsManager will collect logs
In GFI EventsManager event sources are organized into event source groups. The event sources specified below will be added to the 'Servers'.
Add the following computers:
AdminPC
Add
Computer
192.168.3.254
Remove
Select...
Import...
In order to scan a Microsoft Vista or Microsoft Server machine, you must install GFI EventsManager on a Microsoft Vista or Microsoft Server 2008 machine.
< Back
Finish
Cancel

Screenshot 38 - Configuration wizard: Specify the computers that will be monitored

4. Specify the name/IP of the new event source and click **Add**. Repeat until you have specified all the event sources to add to this group.

NOTE: To import the list of event sources from a text file click on the **Import** button. To select event sources from a list, click on the **Select** button.

5. Click **Finish** to finalize your settings. GFI EventsManager will attempt to collects logs from the configured sources immediately after clicking the **Finish** button.

6.3 Configuring event source properties

GFI EventsManager allows you to customize the event source parameters to suit the operational requirements of your infrastructure. You can configure of these parameters on a:

- Computer by computer basis.
- Computer group by group basis.

Event source properties that can be customized include:

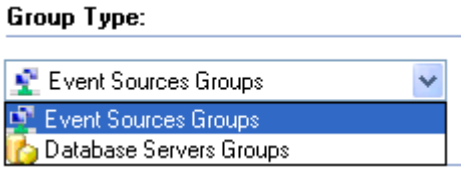
- General event source properties such as computer group name
- Alternative domain administrator credentials required to remotely access the event logs of a target computer.
- Event source operational time. Through these parameters GFI EventsManager can identify key events that occur outside normal operational time such as failed logons. As a result alerts and

notifications can be generated and dispatched to administrators for immediate attention.

- Windows, W3C , SNMP and Syslog event processing parameters.

To configure event source properties:

1. Click on the **Configuration** tab.



Screenshot 39 - Group type

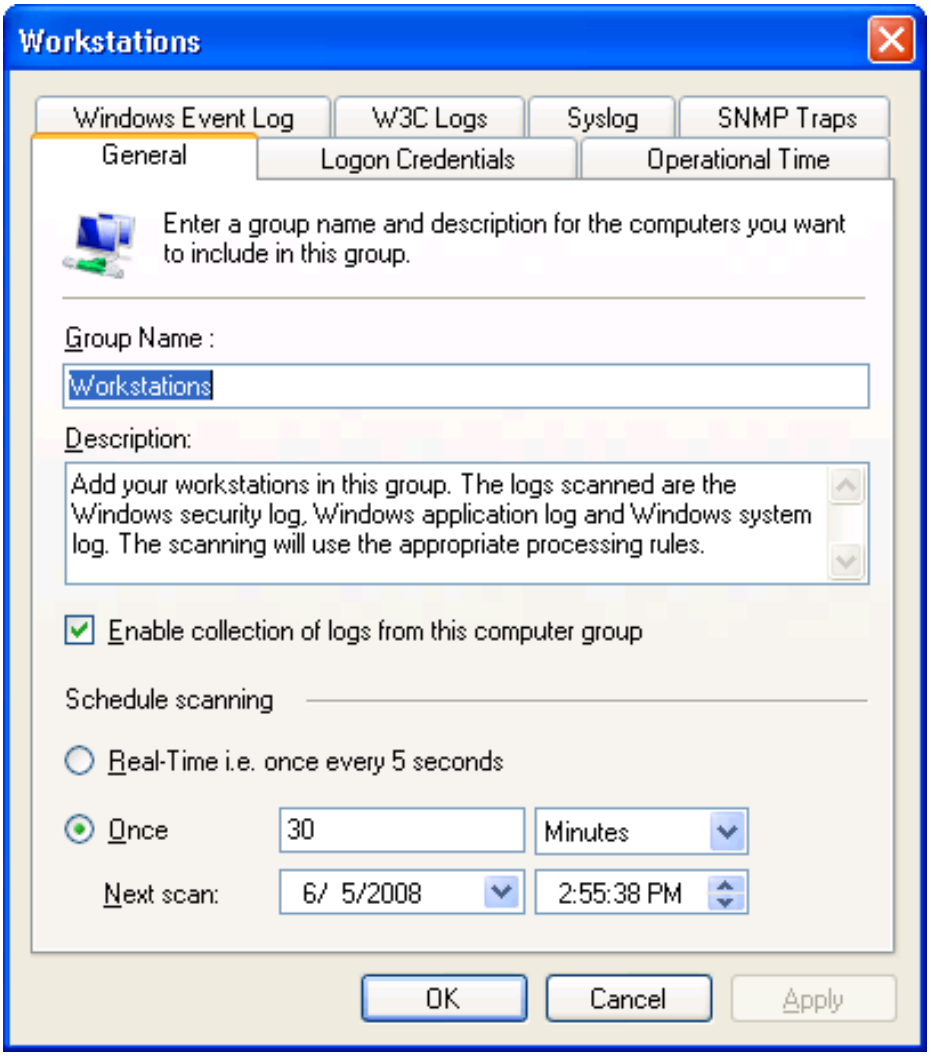
2. From the **Group Type** drop-down select **Event Sources Groups**.

3. To configure the parameters of a:

- Computer group: Right-click on the computer group to be configured and select **Properties**.
- Particular computer in a group:
    - Click on the computer / database server group to which the computer group belongs.
    - From the right pane, right-click on the required computer and select Properties.

4. Click on the required tabs and configure the respective parameters accordingly. More information on how to configure these parameters is provided in the coming sections.

6.3.1 Configuring general event source properties



Screenshot 40 - Event sources properties dialog

Use the **General** tab in the properties dialog to:

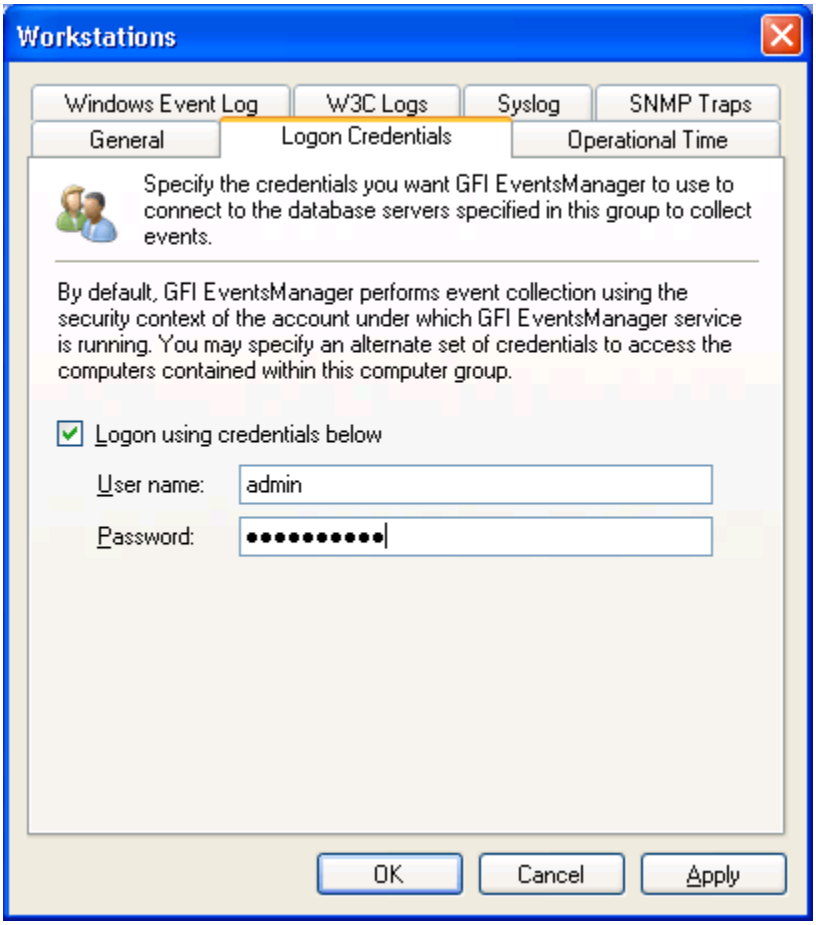
- Change the name of a computer group.
- Enable/disable log collection and processing for the computers in a group.
- Configure log collection and processing frequency.

6.3.2 Configuring alternative domain administrator credentials

During event processing, GFI EventsManager must remotely log-on to the target computers. This is required in order to collect log data that is currently stored on the target computers and to pass this data on to the event processing engine(s).

To collect and process logs, GFI EventsManager must have administrative privileges over the target computers. By default, GFI EventsManager will log-on to target computers using the credentials of the account under which it is currently running; however, certain network environments are configured to use different credentials to log on to workstations and servers with administrative privileges. As an example for security purposes, network administrators can setup a

dedicated account that has administrative privileges over workstations only and a different account that has administrative privileges over servers only.


Workstations
Windows Event Log
W3C Logs
Syslog
SNMP Traps
General
Logon Credentials
Operational Time
Specify the credentials you want GFI EventsManager to use to connect to the database servers specified in this group to collect events.
By default, GFI EventsManager performs event collection using the security context of the account under which GFI EventsManager service is running. You may specify an alternate set of credentials to access the computers contained within this computer group.
Logon using credentials below
User name:
admin
Password:
OK
Cancel
Apply

Screenshot 41 - Configuring alternative logon credentials

GFI EventsManager, allows you to configure a dedicated set of logon credentials for individual target computers as well as for computer groups. To configure a set of credentials for a particular computer group:

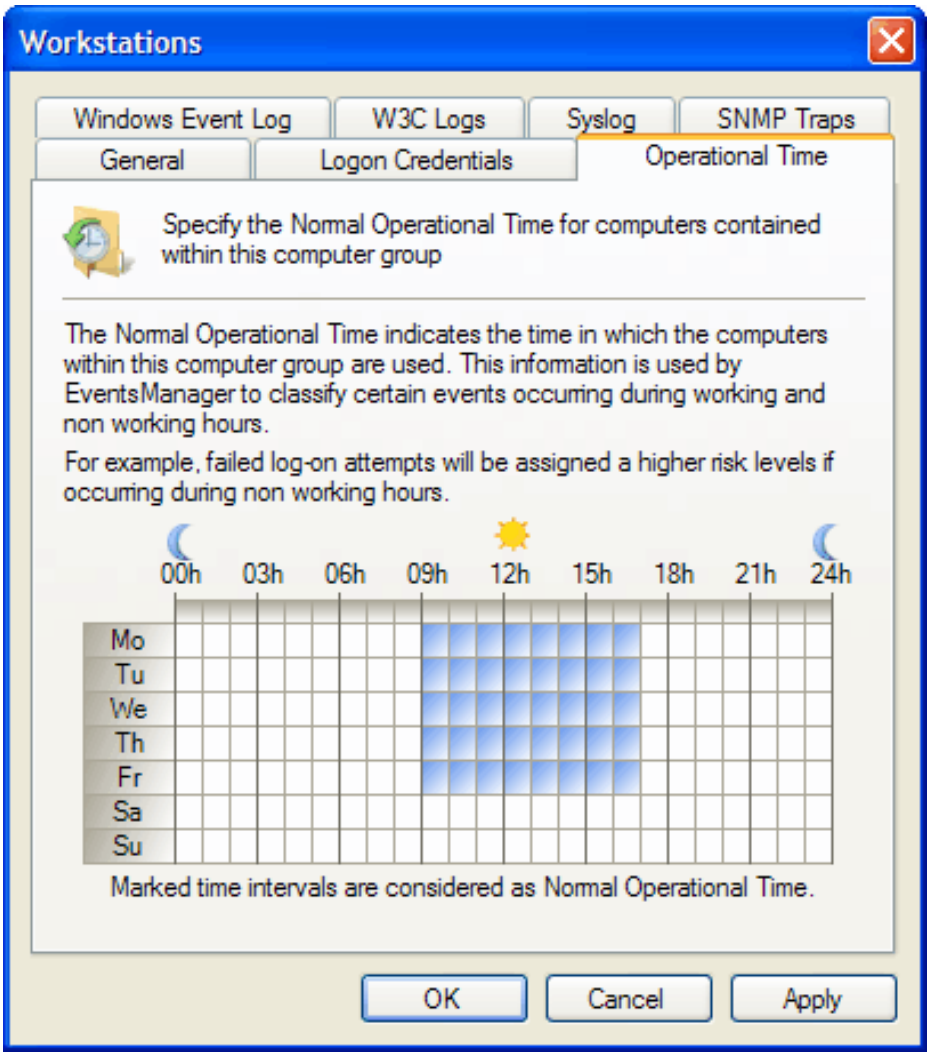
1. Right click on an event source and click on **Properties**

2. Click on the **Logon Credentials** tab

3. Specify the login name and password which will be used to log-on and collect logs from the target computer(s).

6.3.3 Configuring event source operational time

GFI EventsManager includes an **Operational Time** option through which you specify the normal working hours of your event sources. This is required so that GFI EventsManager can keep track of the events that occur both during and outside working hours. Use the operational time information for forensic analysis and to identify network computers that are being misused outside normal working hours. For example, through this information, you can discover unauthorized user access, illicit transactions carried out outside normal working hours and other potential security breaches that might be taking place on your network.

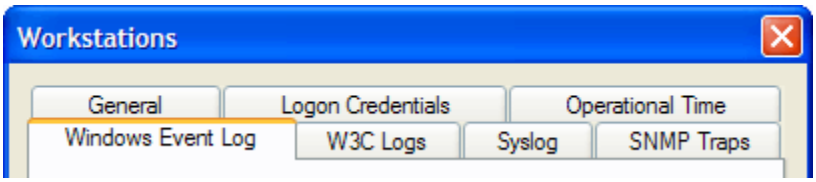


Screenshot 42 - Specify operational time

Operational time is configurable on computer group basis. Configuration is achieved through the **Operational Time** tab provided in the computer group properties; Operational time is configured by marking the normal working hours on a graphical operational time scale which is divided into 1 hour segments.

6.3.4 Configuring event processing parameters

To configure event processing parameters:



Screenshot 43 - Event-processing configuration tabs

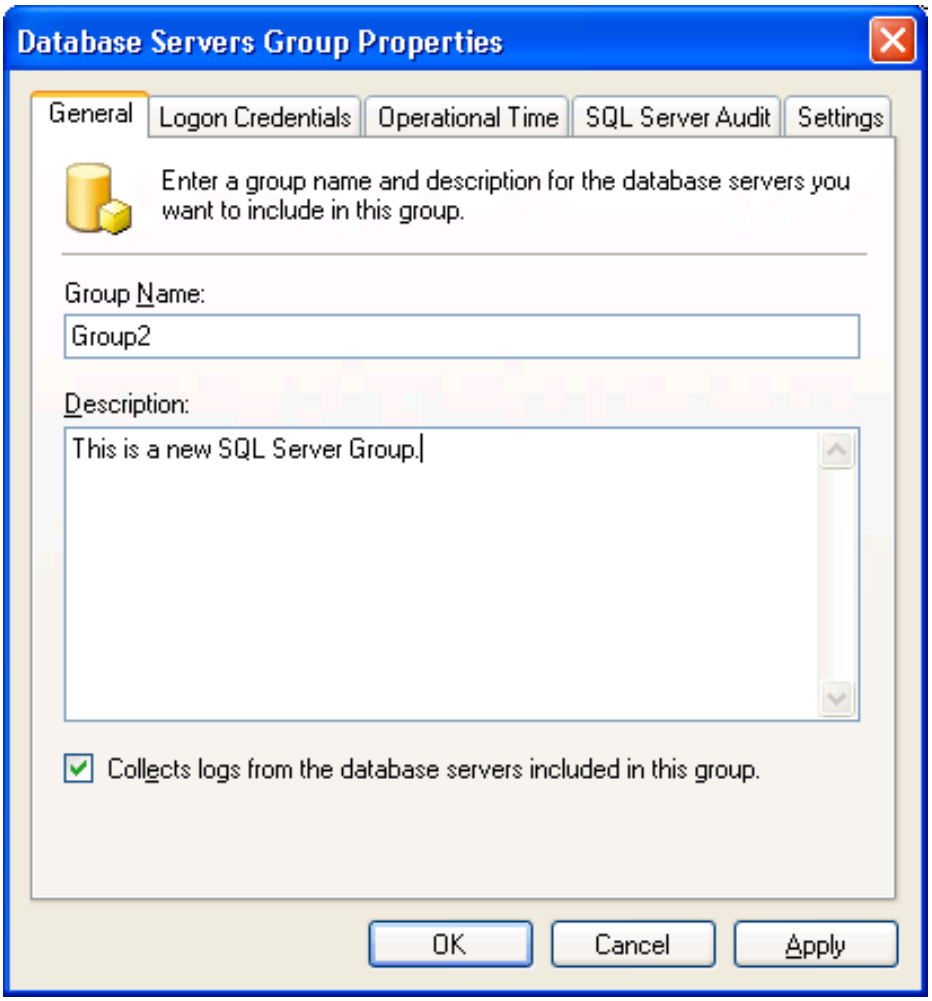
1. Bring up the (computer/computer group) properties dialog

2. Use the **Windows Event Log** tab, **W3C Logs** tab, **Syslog** tab and **SNMP Traps** to configure the required event processing parameters. For more information on how to configure these parameters refer to the 'Configuring event processing rules' chapter.

6.4 Adding a new SQL Servers group

1. Click on the **Configuration** tab.

2. From the **Group Type** drop-down select **Database Servers Groups**.



Screenshot 44 - Creating a new SQL Server group

3. Right-click on an existing group and select **Create group.**

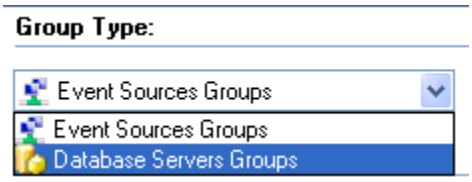
4. Configure the SQL Server group settings. For more information about SQL Server group configuration, refer to the section 'Configuring SQL Server group properties' in this chapter.

6.5 Configuring SQL Servers event source properties

Similar to group properties both in concept as well as in terms of configuration, SQL Servers event source properties can be configured at both group level and individual SQL Server level.

To configure the properties of an individual SQL Server or server group

1. Click on the **Configuration** tab.



Screenshot 45 - Database Servers Groups

2. From the **Group Type** drop-down select **Database Server Groups.**

3. To configure the parameters of a:

- Database Server Group: Right-click on the database server/ group to be configured and select **Properties**.
- Particular computer in a database server group: Click on the database server group to which the computer group belongs. Then from the right pane, right-click on the required computer and select **Properties**.

4. Use the tabs provided in the properties dialog, to configure the required parameters:

- **General properties:** Use this tab to change the group name.
- **Logon credentials:** Use this tab to select the authentication method to be used and if required specify login credentials.
- **Operational time:** Use this tab to specify the operational time for the database servers specified in this group.
- **SQL Server audit:** Use this tab to configure which event processing rules will be applied against the events collected from source. By default, GFI EventsManager is set to inherit these parameters from the parent Database Server Group.
- **Settings:** Use this tab to configure SQL Server event-scanning options (i.e. scan all databases, scan security events only on all databases or scan only a specific database).

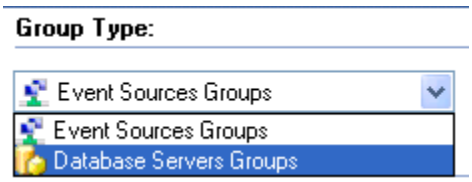
NOTE: For more information on how to configure these parameters please refer to the 'Configuring SQL Servers group properties' section in this chapter.

6.6 Adding new SQL Servers to the default group

The SQL Server audit feature allows you to process the activity logs generated by day-to-day SQL Server operations such as server startup or on key events such as failed logons.

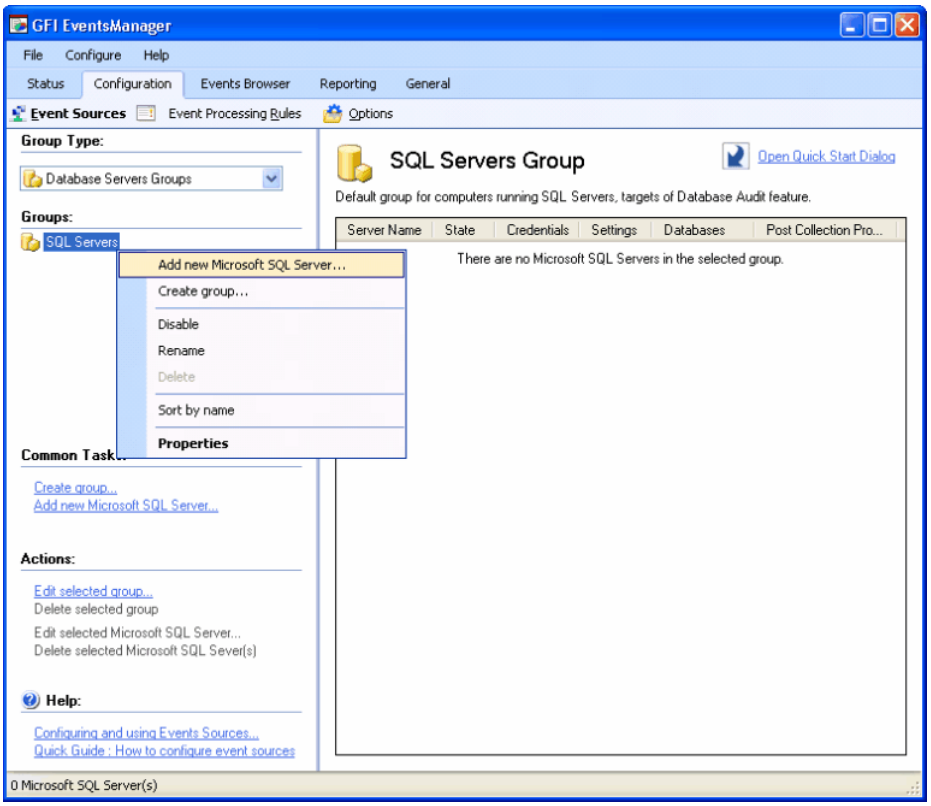
Like computers, SQL Servers can be grouped and processed using a common event-log scanning policy. To create an SQL Server group:

1. Click on the **Configuration** tab.



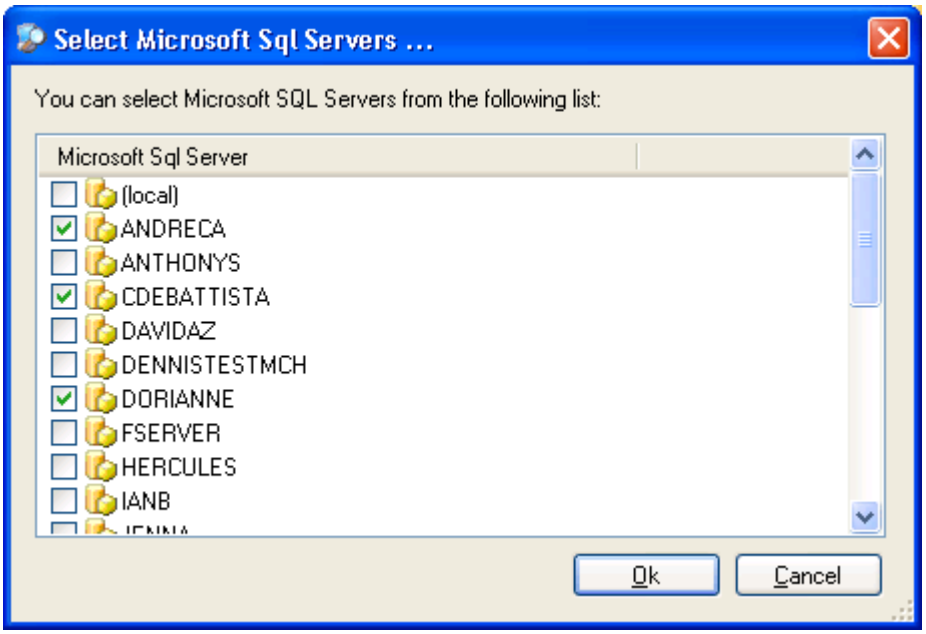
Screenshot 46 - Database Servers Groups

2. From the **Group Type** drop-down select **Database Servers Groups**.



Screenshot 47 - Add a new Microsoft SQL Server

3. In the **Groups** section, right click on **SQL Servers** and select **Add new Microsoft SQL Server**.



Screenshot 48 - Select Microsoft SQL Server(s)

4. Click on the **Select** button and choose the required Microsoft SQL Server machines from list. Click **OK** when selection is complete.

5. Click on the **Finish** button to finalize your settings.

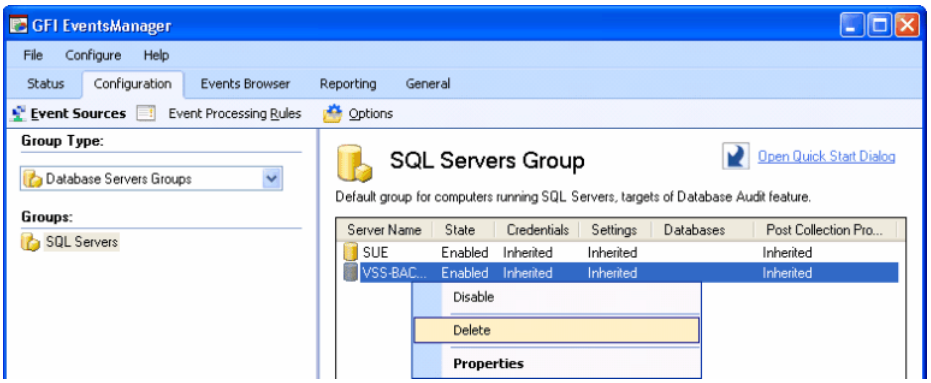
NOTE: You cannot audit the SQL Server that is currently being used as database backend by GFI EventsManager.

6.7 Removing SQL Servers from the default group

To remove a Database Server Group:

1. Click on the **Configuration** tab.

2. From the **Group Type** drop-down select **Database Servers Groups**.



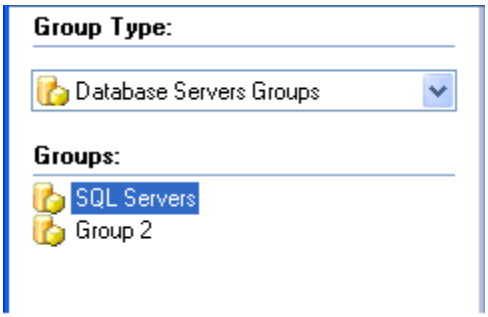
Screenshot 49 - Select Microsoft SQL Server to delete

3. In the right pane, right click on the SQL Server to be deleted and select **Delete**.

6.8 Configuring database server properties

By default, an SQL Server will inherit the properties that were set for the parent group settings (for example the 'SQL Servers' group). To change these settings for a specific server:

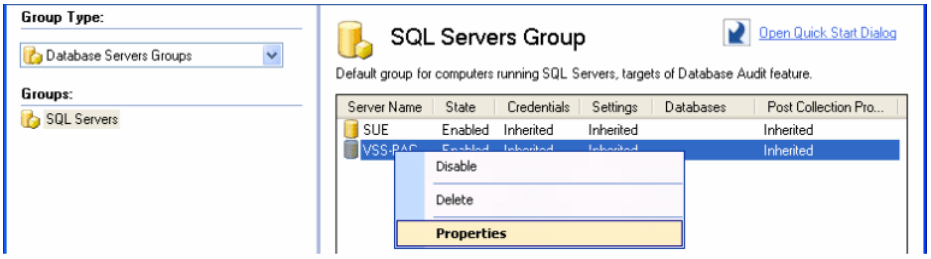
1. Click on the **Configuration** tab.



Screenshot 50 - 'SQL Servers' Group

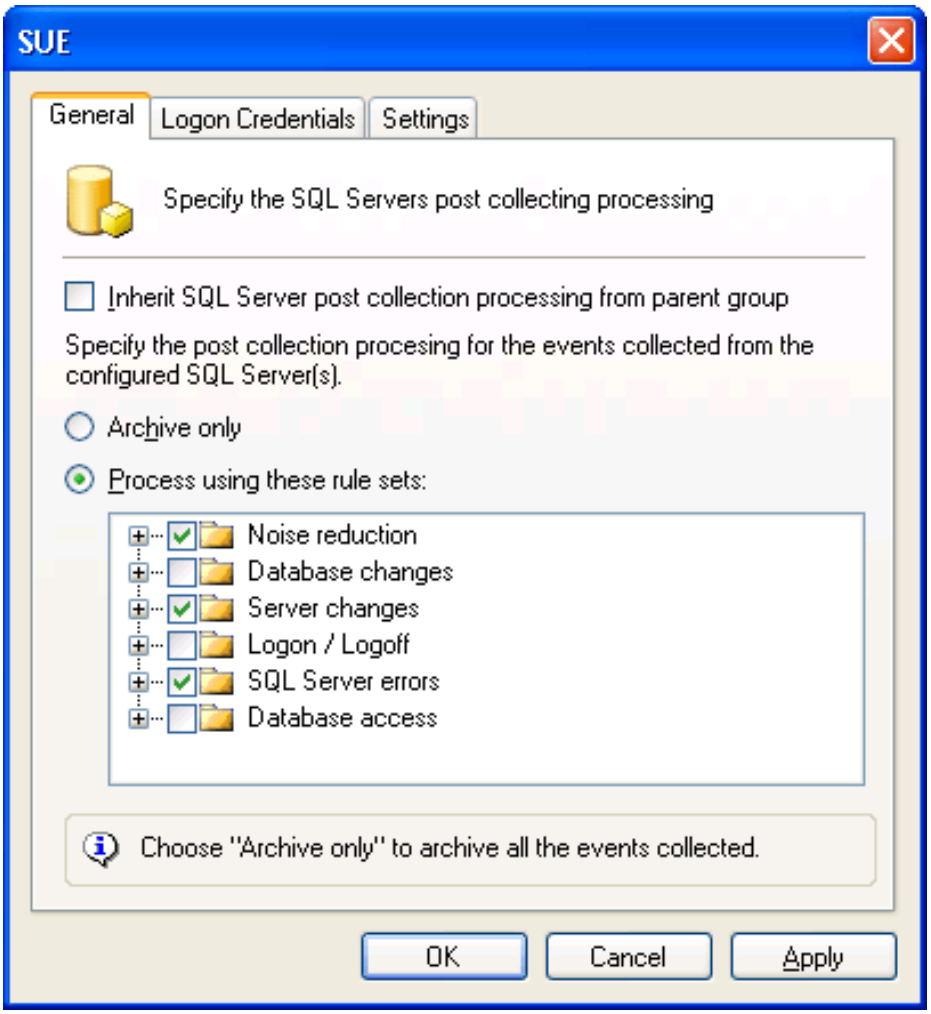
2. From the **Group Type** drop-down select **Database Servers Groups**.

3. From the **Groups** area, select the group that contains the SQL Server that you would like to edit, for example 'SQL Servers'.



Screenshot 51 - Microsoft SQL Server group properties

3. In the left pane, right click on the Microsoft SQL Server to be configured and select **Properties**. This will bring up the SQL Servers Group properties dialog.



Screenshot 52 - The SQL Server Group properties dialog

4. Use the tabs provided in this dialog as follows:

- **General tab:** Use this tab to set post collection processing rules. By default, GFI EventsManager will inherit post collection processing from the parent group.
- **Logon credentials:** Use this tab to select the authentication method to be used and to specify login credentials if 'SQL Server Authentication' will be used.
- **Settings:** Use this tab to configure SQL Server event-scanning options (i.e. scan all databases, scan security events only on all databases or scan only a specific database).

NOTE: For more information on how to configure these parameters please refer to the 'Configuring SQL Servers group properties' section in this chapter.

7 Configuring event processing rules

7.1 Introduction

GFI EventsManager allows you to collect and process: Windows Event Logs, W3C logs, Syslogs, SNMP Traps and Microsoft SQL Server audit logs. All supported log types record events in a different and proprietary format; therefore every log type requires different configuration settings and parameters. You can configure log collection and processing parameters:

- On a computer by computer basis
- On a computer group by computer group basis.

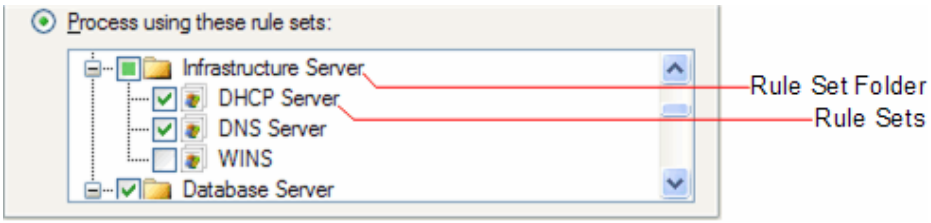
During event processing, GFI EventsManager runs a configurable set of rules against the collected logs in order to classify events and trigger alerts/actions accordingly. By default, GFI EventsManager ships with a pre-configured set of event processing rules that allow you to gain network-wide control over computer logs - with negligible configuration effort.

Event processing rules

Event processing rules are instructions/checks that:

- Analyze the collected logs.
- Classify the severity of processed events. Classification is based on the configuration settings of the processing rule.
- Filter events that match specific criteria. For example, you can create and run a rule which filters out low severity events and noise (duplicate events).
- Generate alerts and actions based on event severity. For example, you can configure GFI EventsManager to send both SMS and Email alerts whenever an event is classified as critical; but limit the product to send only email alerts when an event is classified as high in severity. For more information on how to configure alerts and actions refer to the 'Configuring alerting and actions' chapter.
- Optionally archive filtered events. Event archiving is based on the severity of the event and on the configuration settings of the event processing rules. For example, you can configure GFI EventsManager to archive only events that are classified critical or high in severity and discard all the rest.

In GFI EventsManager, event processing rules are organized into 'Rule-sets'; and every rule-set can contain one or more specialized rules which can be run against collected logs.



Screenshot 53 - Rule-sets folder and Rule-sets

Rule-sets are further organized into 'Rule-sets Folders'. This way you can group rule-sets according to the functions and actions that the respective rules perform. By default, GFI EventsManager ships with pre-configured folders, rule-sets and event processing rules that can be further customized to suite your event processing requirements.

Event classification

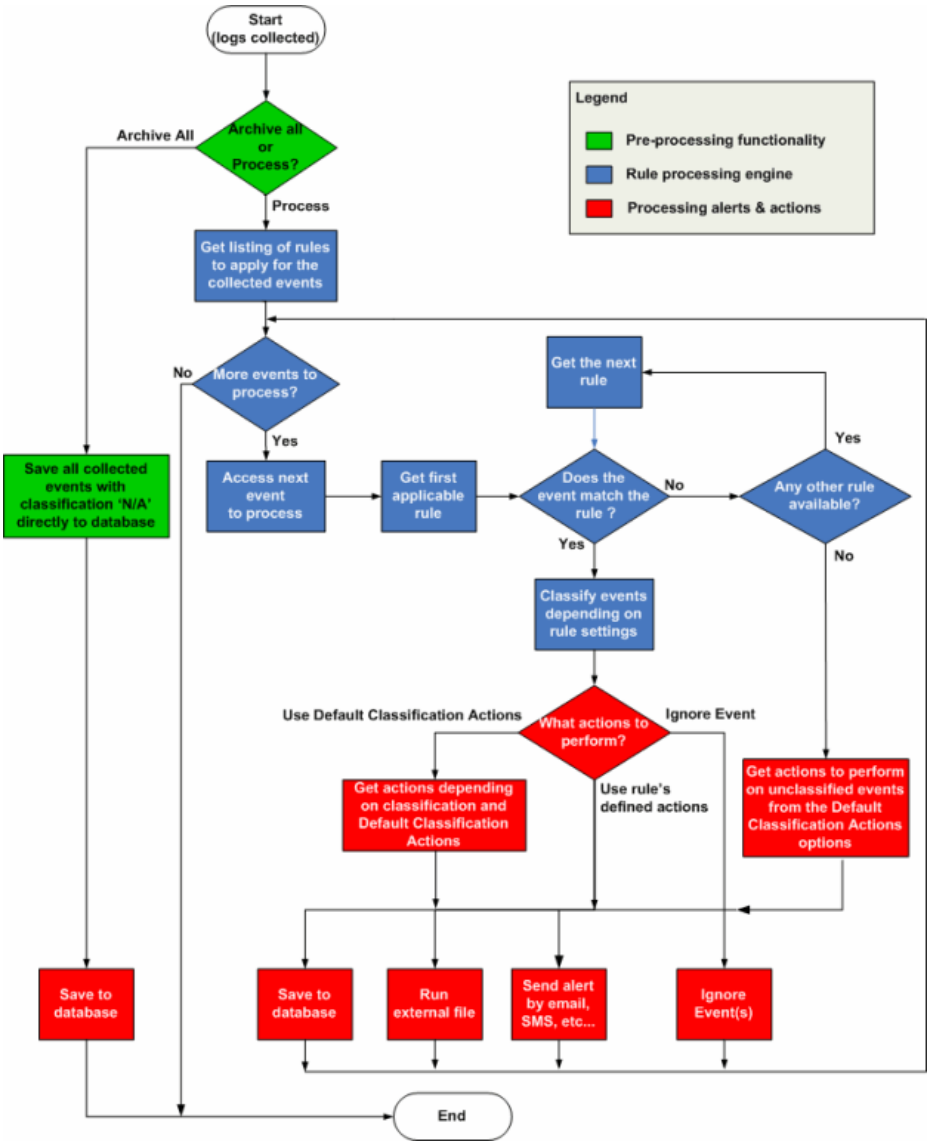
GFI EventsManager classifies events in 5 categories:

- Critical
- High
- Medium
- Low
- Noise (unwanted or repeated log entries).

Event classification is based on the configuration of the rules that are executed against the collected logs. Events that don't satisfy any event classification conditions are tagged as unclassified and can be set to trigger the same alerts and actions available for classified events.

Event processing, classification and actions flowchart

The flowchart chart below illustrates the event processing stages performed by GFI EventsManager.

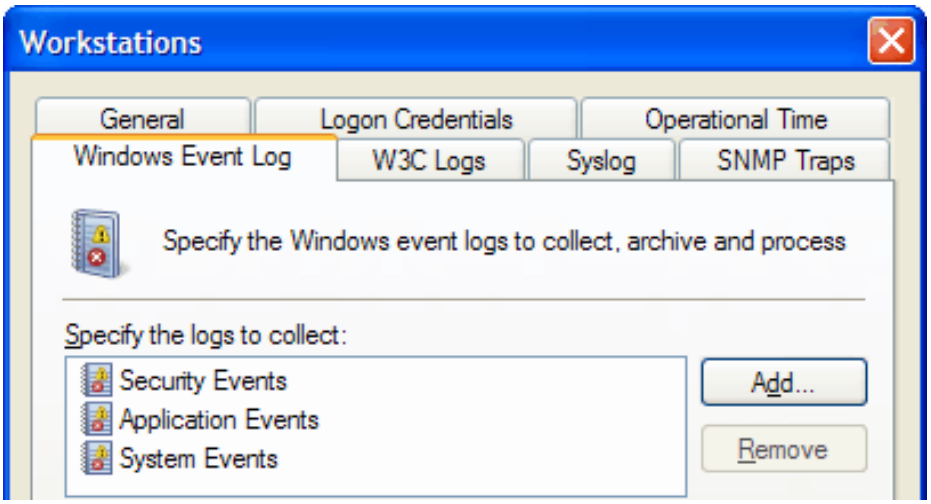


Screenshot 54 - Log processing, classification and actions flowchart

7.2 Collecting and processing Windows events

Overview

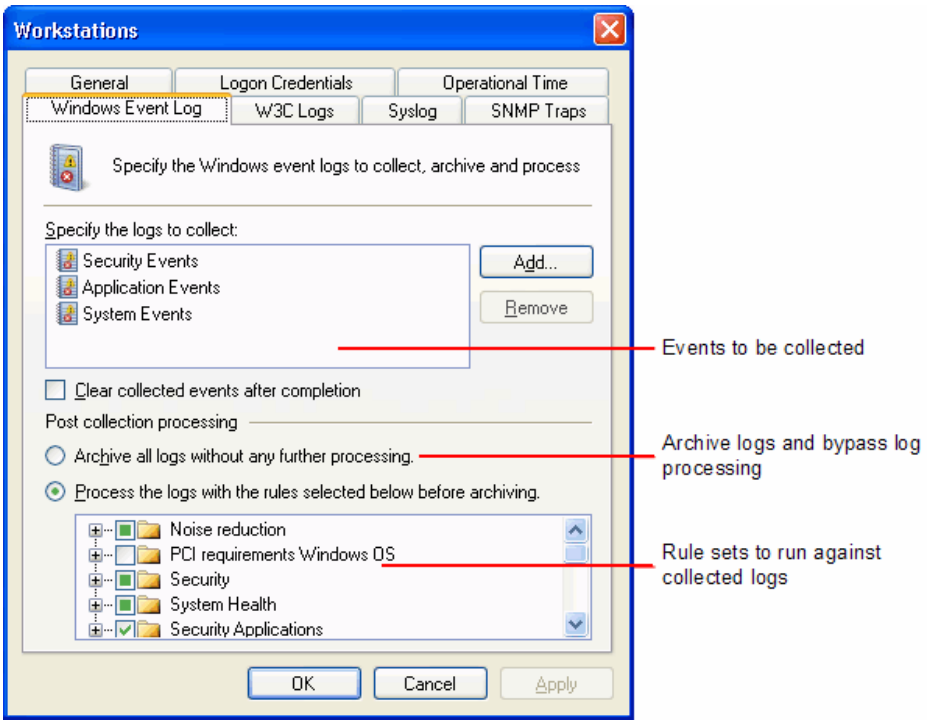
Windows events are organized into specific log categories; by default computers running on Windows NT or higher record errors, warnings and information events in 3 logs namely Security, Application and System logs. Computers that have more specialized roles on the network (e.g. Domain Controllers, DNS Servers, etc.) have additional event log categories.



Screenshot 55 - Computer group properties: Configuring logs to be processed

As a minimum, Windows Operating Systems record events in the following logs:

- **Security events log:** This log contains security related events through which you can audit successful or attempted security breaches. Typical events found in the Security Events log include valid and invalid logon attempts.
- **Application events log:** This log contains events recorded by software applications/programs such as file errors.
- **System events log:** This log contains events logged by Windows XP system components such as failures to load device drivers.
- **Directory service log:** This log contains events generated by the Active Directory including successful or failed attempts to make to update the Active Directory database.
- **File Replication service log:** This log contains events recorded by the Windows File Replication service. These including file replication failures and events that occur while domain controllers are being updated with information about sysvol.
- **DNS server log:** This log contains events associated with the process of resolving DNS names to IP addresses.
- **Application and Services Logs:** These logs contain events associated with Windows VISTA and the relative services/functionalities it offers.



Screenshot 56 - Computer group properties: Configuring Windows Event Logs parameters

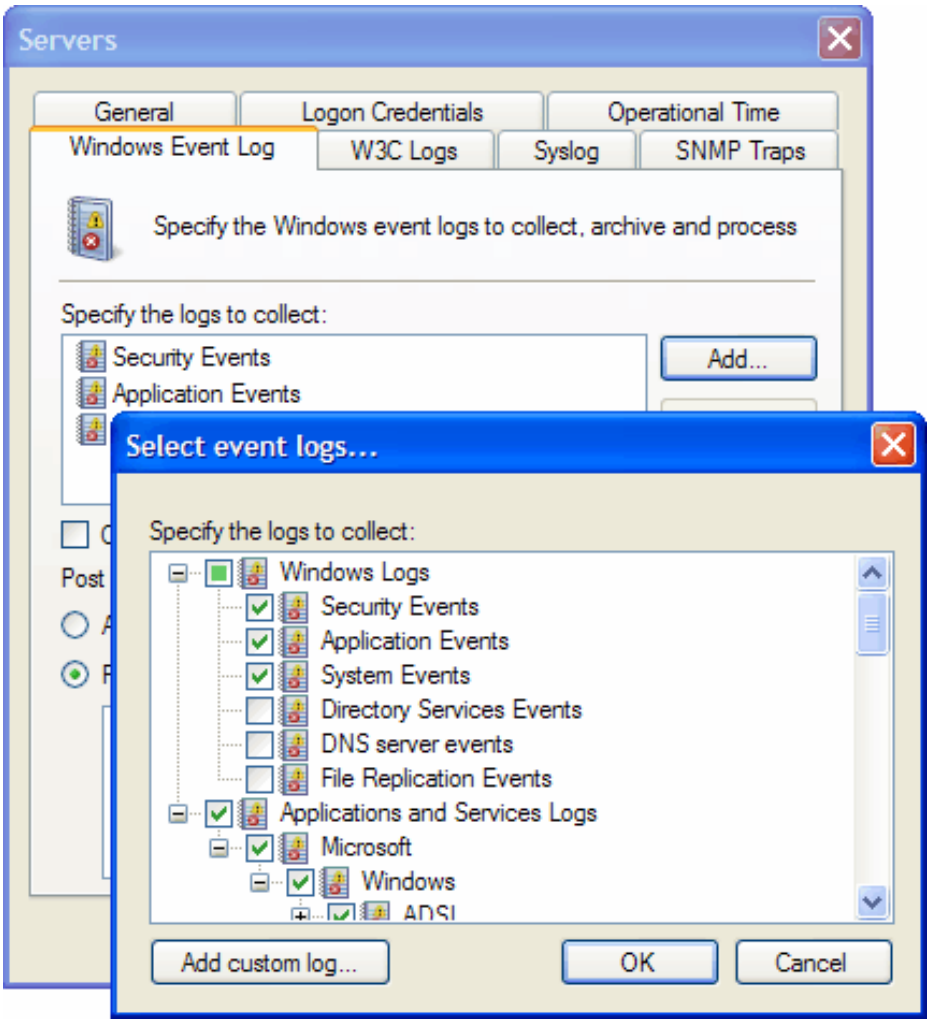
To configure Windows Event Log collection and processing parameters you must:

- Select the events to be collected.
- Specify whether the collected logs will be processed (filtered, etc.) or just archived without processing.
- Select the event processing rule-sets/rules that will be run against the collected logs.

Selecting the events to be collected

To specify which Windows events will be collected by GFI EventsManager:

1. Bring up the (computer/computer group) properties dialog.
2. Click on the **Windows Event Log** tab.



Screenshot 57 - Selecting the events to be collected

3. Click on **Add** and select the check-box of the events that will be collected.

NOTE: GFI EventsManager supports custom event logs. For information on how to configure custom event logs please refer to the 'Configuring Custom Event Logs' section in this chapter.

4. (Optionally) Select the option 'Clear collected events after completion' to clear the collected events from event sources.

IMPORTANT: Deleting events from source logs without having them archived or backed-up may lead to legal compliance issues. Please make sure to archive or backup important events according to the standards implied by data retention and data protection regulations.

Archiving Windows events

For information on how to archive events refer to the 'Archiving events' section in this chapter.

Selecting Windows event processing rules

For information on how to select event processing rules refer to the 'Selecting event processing rules' section in this chapter.

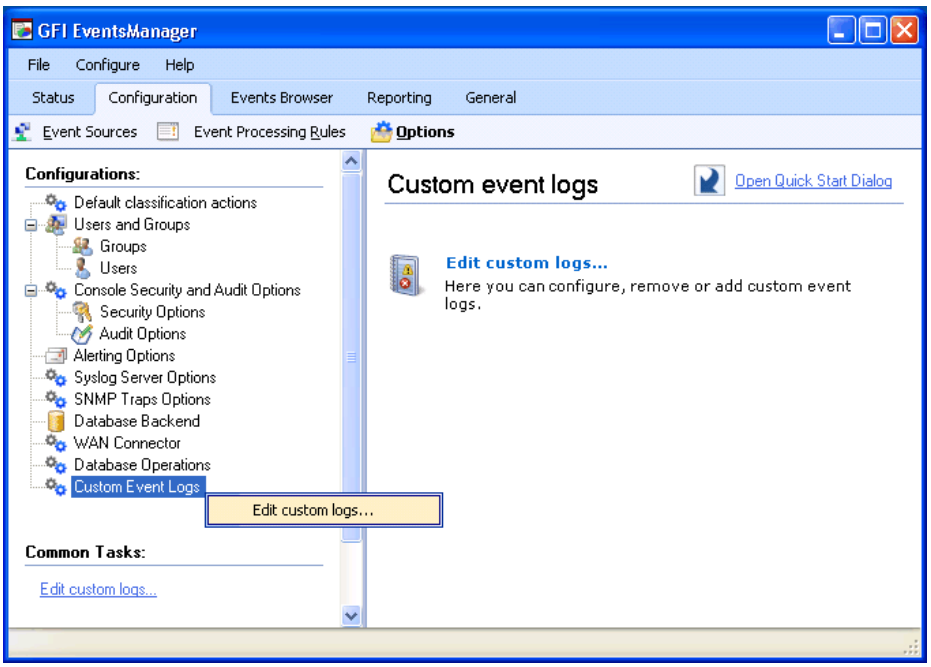
7.3 Configuring custom event logs

GFI EventsManager is configured to collect and process standard Windows Event Logs. However, GFI EventsManager can also be configured to manage events recorded in third party application logs such as anti-virus logs, software firewall logs and other security software.

To configure custom events:

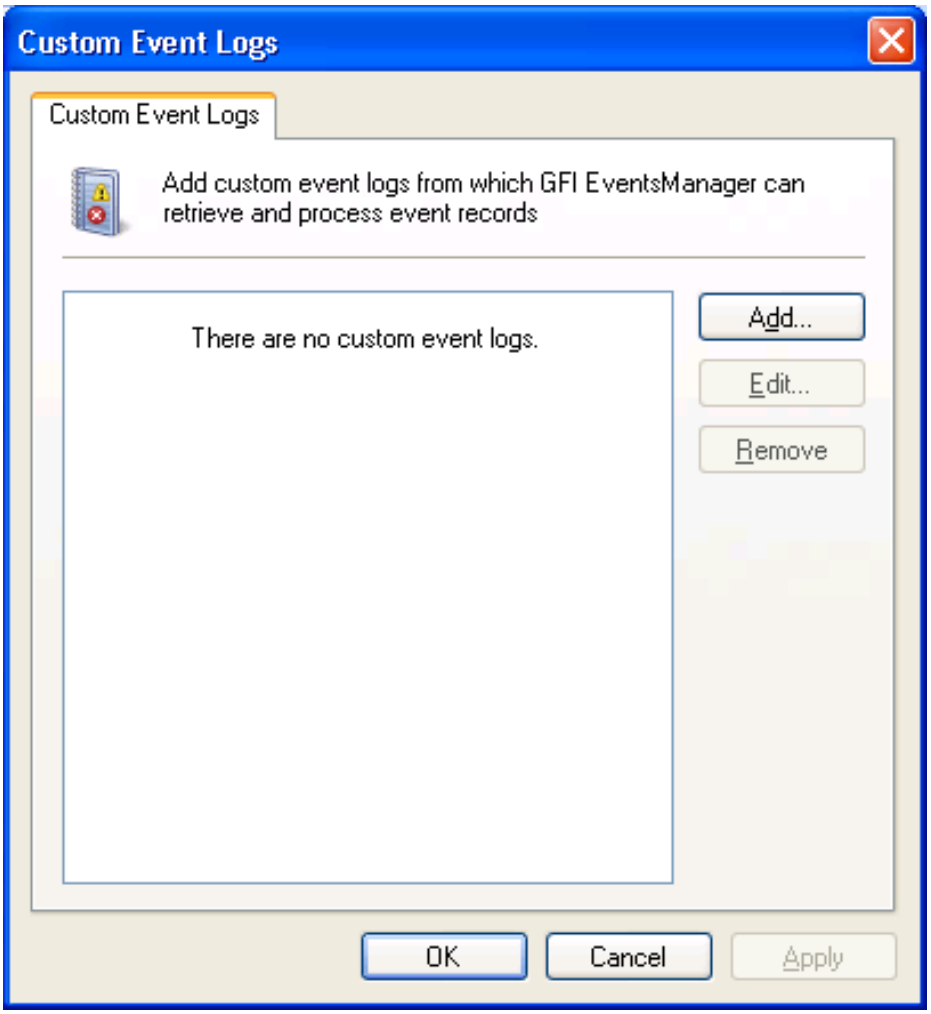
1. Click the Configuration tab and select Options.

2. From the left pane, right-click on the **Custom Events Logs** node and select **Edit custom logs…**



Screenshot 58 - Custom event logs setup

3. Click on the **Add…** button and specify the name of your custom event log.



Screenshot 59 - Custom event logs dialog

4. Click **OK** to finalize your settings.

7.4 Collecting and processing W3C logs

W3C is another log format supported by GFI EventsManager. W3C logs are text-based flat files containing various event details delimited by special characters.

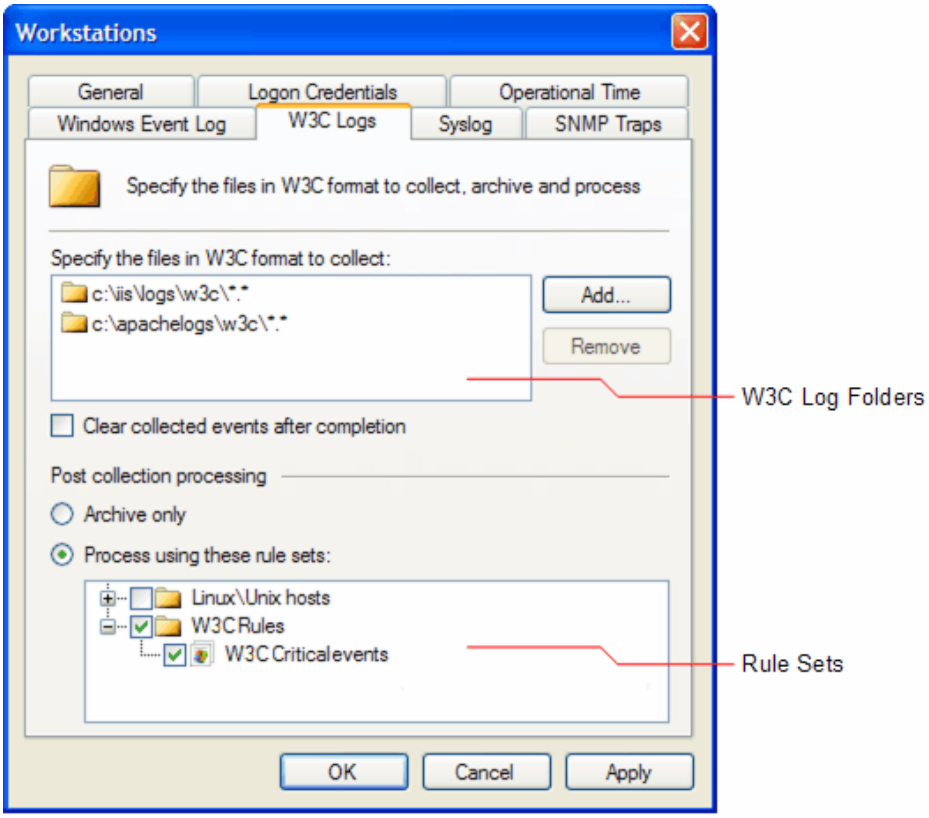
The W3C log format is mostly commonly used by hardware systems (e.g. servers and appliances) which have internet specific roles. Microsoft Internet Information Server (IIS) service and Apache web servers for example, can collect web related events (i.e. web logs) in the form of W3C formatted text files.

In GFI EventsManager, the configuration process of W3C log parameters is identical to that performed for Windows event processing, with one exception. Unlike Windows Event Logs, there is no standard which dictates a specific or centralized folder location where W3C log files are stored on disk. Therefore, in order to collect W3C logs, you must specify the complete path to these text-based log files.

Selecting the events to be collected and processed

To specify which W3C logs will be collected by GFI EventsManager:

1. Bring up the (computer/computer group) properties dialog.
2. Click on the **W3C Log** tab.



Screenshot 60 - Computer group properties: Configuring W3C event processing parameters

3. Click on **Add** and specify the log file name and location. Wildcards such as *.* are supported.

4. (Optionally) Select the option 'Clear collected events after completion' to clear the collected events from event sources.

IMPORTANT: Deleting events from source logs without having them archived or backed-up may lead to legal compliance issues. Please make sure to archive or backup important events according to the standards implied by data retention and data protection regulations.

Archiving W3C events

For information on how to archive events refer to the 'Archiving events' section in this chapter.

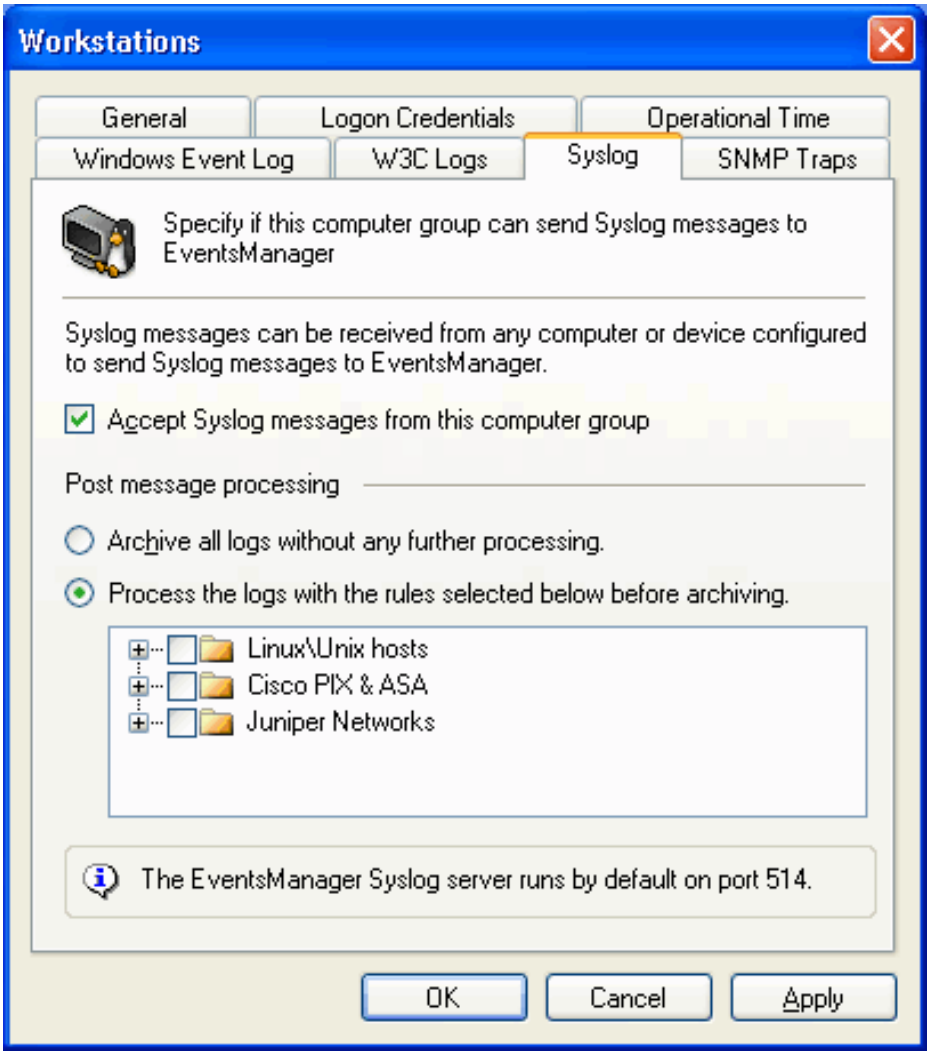
Selecting W3C event processing rules

For information on how to select event processing rules refer to the 'Selecting event processing rules' section in this chapter.

7.5 Collecting and processing Syslogs

Syslog is a data logging service that is most commonly used in Linux and UNIX based environments. The concept behind Syslogs is that the logging of events and information is entirely handled by a dedicated server called 'Syslog Server'. This means that unlike Windows and W3C log based environments, regular programs do not

log any information. They just send events in the form of data messages (technically known as 'Syslog Messages') to a Syslog server that will manage the message and save the data in a log file.


Workstations
General
Logon Credentials
Operational Time
Windows Event Log
W3C Logs
Syslog
SNMP Traps
Specify if this computer group can send Syslog messages to EventsManager
Syslog messages can be received from any computer or device configured to send Syslog messages to EventsManager.
Accept Syslog messages from this computer group
Post message processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
Linux\Unix hosts
Cisco PIX & ASA
Juniper Networks
The EventsManager Syslog server runs by default on port 514.
OK
Cancel
Apply

Screenshot 61 - Computer group properties: Syslog processing parameters

In order to process Syslog messages, GFI EventsManager ships with a built-in Syslog Server. This Syslog server will automatically collect, in real-time, all Syslog messages/events sent by Syslog sources and pass them on to the event processing engine. Out-of-the-box GFI EventsManager supports events generated by various network devices manufactured by leading providers including Cisco and Juniper. For more information about supported devices visit: http://kbase.gfi.com/showarticle.asp?id=KBID002868.

A built-in buffer allows the Syslog server to collect, queue and forward up to 30 Syslog messages for batch processing. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at 1 minute intervals whichever comes first.

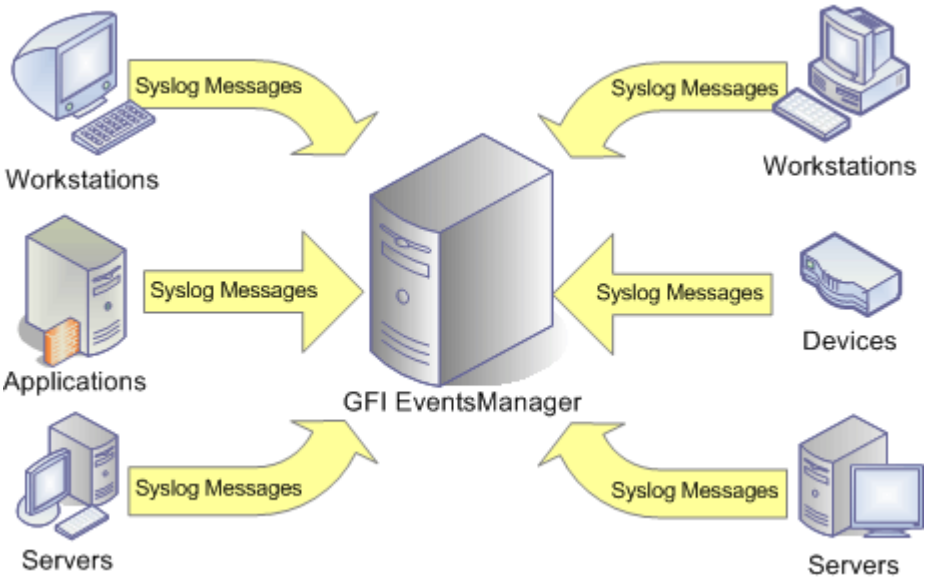


Figure 6 - Syslog messages must be directed to the computer running GFI EventsManager

NOTE: For Syslog message processing, ALL Syslog sources (e.g. workstations, servers, network appliances, etc.) must be configured to send their messages to the computer/IP where GFI EventsManager is installed. This applies also for the computer that is running GFI EventsManager.

In GFI EventsManager, Syslog event processing parameters are configured as follows:

1. Open up the (computer/computer group) properties dialog.

2. Click on the **Syslog** tab.

3. To enable the Syslog server and listen for messages sent by the computers in a computer group, select the option 'Accept Syslog Messages from this computer group'.

IMPORTANT: Deleting events from source logs without having them archived or backed-up may lead to legal compliance issues. Please make sure to archive or backup important events according to the standards implied by data retention and data protection regulations.

NOTE 1: The GFI EventsManager Syslog server is by default configured to listen for Syslog messages on port 514. For more information on how to customize Syslog server port settings refer to the 'Configuring Syslog server communications port' section in this chapter.

NOTE 2: The built-in Syslog server will only accept Syslog messages sent from the computers that are part of this computer group.

Archiving Syslog events

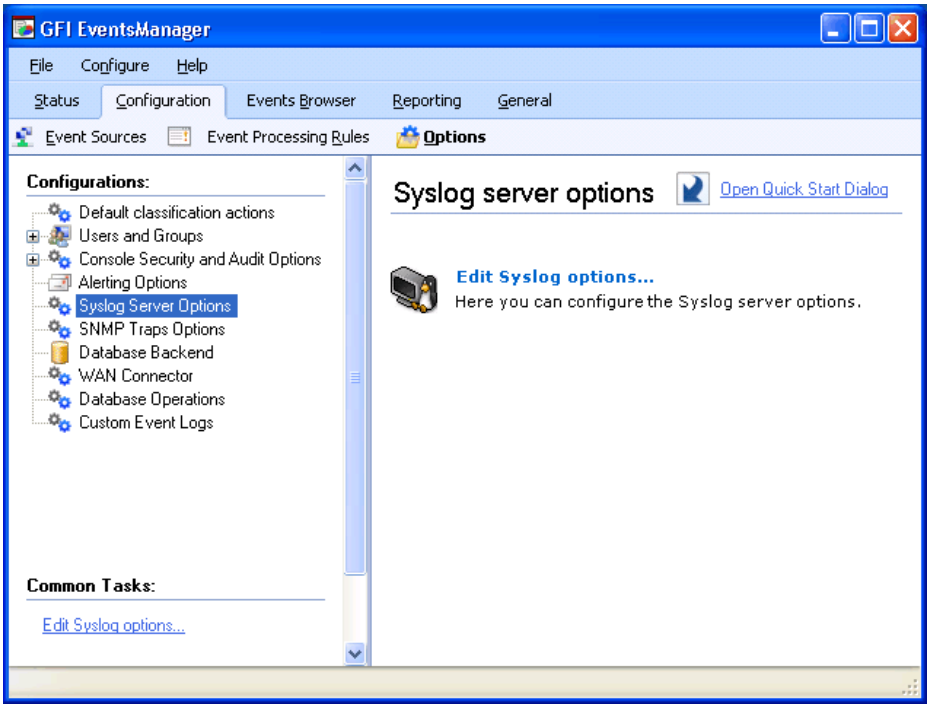
For information on how to archive events refer to the 'Archiving events' section in this chapter.

Selecting Syslog processing rules

For information on how to select event processing rules refer to the 'Selecting event processing rules' section in this chapter.

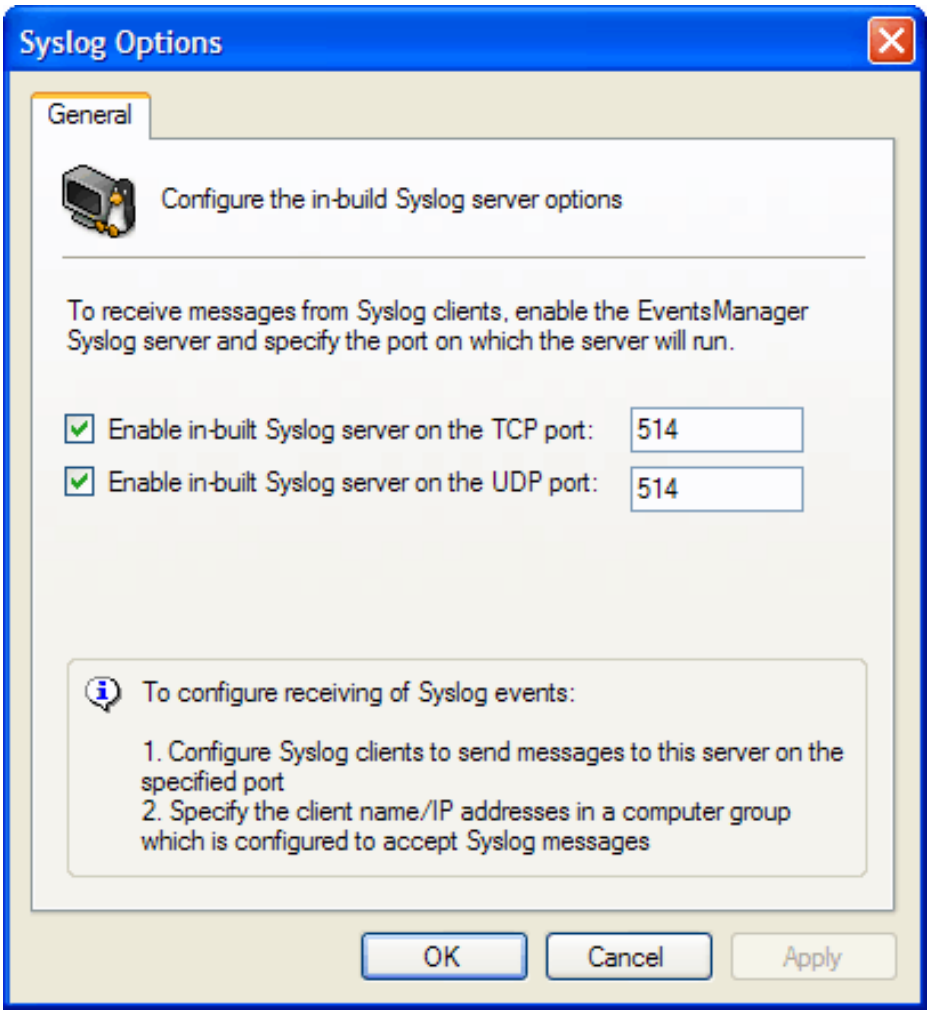
7.6 Configuring the Syslog server communications port

To change the default Syslog ports settings:



Screenshot 62 - Configuring Syslog Server

1. Select **Configuration** tab
2. Select **Options** from the tab options.
3. From the left pane, right-click the **Syslog Server Configuration** node and select **Edit Syslog options…**


Syslog Options
General
Configure the in-build Syslog server options
To receive messages from Syslog clients, enable the EventsManager Syslog server and specify the port on which the server will run.
Enable in-built Syslog server on the TCP port:
514
Enable in-built Syslog server on the UDP port:
514
To configure receiving of Syslog events:
1. Configure Syslog clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept Syslog messages
OK
Cancel
Apply

Screenshot 63- Syslog server properties

4. Select **Enable in-built Syslog server on TCP / UDP port:** and specify the TCP/UDP port on which GFI EventsManager will receive/listen for Syslog messages.

5. Select **OK** to finalize your settings.

NOTE: When configuring Syslog server port settings, make sure that the configured port is not already in use by other installed applications. This may affect the delivery of Syslog messages to GFI EventsManager.

7.7 Collecting and processing SNMP Traps

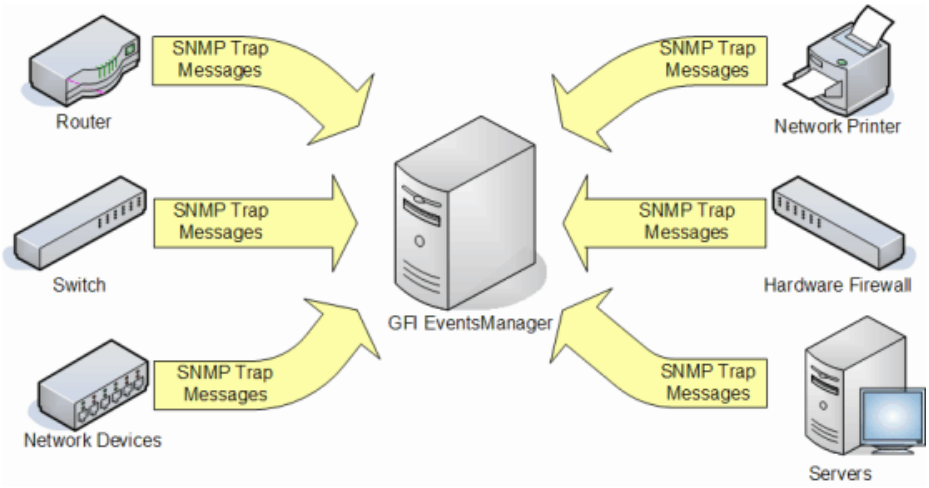
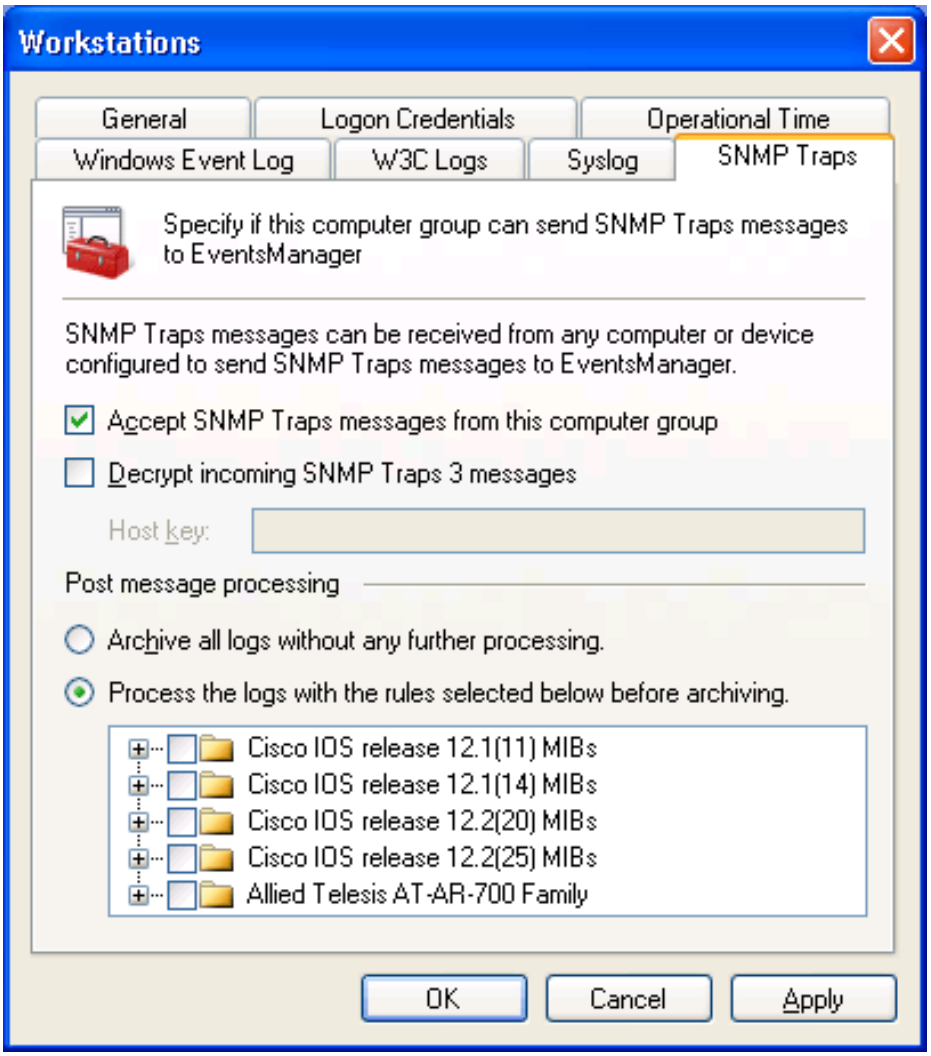


Figure 7: SNMP Trap messages must be directed to the computer running GFI EventsManager

SNMP is a data logging service that enables networked devices to log events and information through data messages (technically known as SNMP Traps). SNMP messaging technology is similar in concept to Syslogs - where unlike Windows and W3C log based environments, devices that generate SNMP messages do not record events data in local logs. Instead events information is sent in the form of data messages to an SNMP Trap Server which manages and saves SNMP message data in a local (centralized) log file.

GFI EventsManager natively supports an extensive list of SNMP devices and Management Information Bases (MIBs). For a full list of supported devices visit:
http://kbase.gfi.com/showarticle.asp?id=KBID002868.


Workstations
General
Logon Credentials
Operational Time
Windows Event Log
W3C Logs
Syslog
SNMP Traps
Specify if this computer group can send SNMP Traps messages to EventsManager
SNMP Traps messages can be received from any computer or device configured to send SNMP Traps messages to EventsManager.
Accept SNMP Traps messages from this computer group
Decrypt incoming SNMP Traps 3 messages
Host key:
Post message processing
Archive all logs without any further processing.
Process the logs with the rules selected below before archiving.
Cisco IOS release 12.1(11) MIBs
Cisco IOS release 12.1(14) MIBs
Cisco IOS release 12.2(20) MIBs
Cisco IOS release 12.2(25) MIBs
Allied Telesis AT-AR-700 Family
OK
Cancel
Apply

Screenshot 64 - Computer group properties: SNMP processing parameters

GFI EventsManager includes a dedicated SNMP Trap Server through which SNMP Traps are handled. A built-in buffer allows the SNMP Trap Server to collect, queue and forward up to 30 SNMP Trap messages for batch processing. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at 1 minute intervals whichever comes first.

NOTE: For SNMP Trap processing, ALL sources (e.g. workstations, servers, network appliances, etc.) must be configured to send their messages to the computer/IP where GFI EventsManager is installed. This applies also for the computer that is running GFI EventsManager.

To configure SNMP processing parameters

1. Open the computer/computer group properties dialog.

2. Click on the **SNMP Traps** tab.

3. To listen to SNMP messages via built-in SNMP Trap Server select the 'Accept SNMP Traps messages from this computer group' option.

IMPORTANT: Deleting events from source logs without having them archived or backed-up may lead to legal compliance issues.

NOTE 1: The GFI EventsManager SNMP Trap Server is by default configured to listen for SNMP Trap messages on port 162. For more information on how to customize SNMP Trap Server port settings refer

to the ‘Configuring the SNMP Trap server settings’ section in this chapter.

NOTE 2: The built-in SNMP Trap Server will only accept SNMP messages sent from the computers that are part of this computer group.

NOTE 3: The built in SNMP Trap Server supports SNMP version 3 Traps with encryption. For encrypted SNMP messages the encryption host key must be provided in the decrypt incoming SNMP Traps 3 message field.

Archiving SNMP Trap events

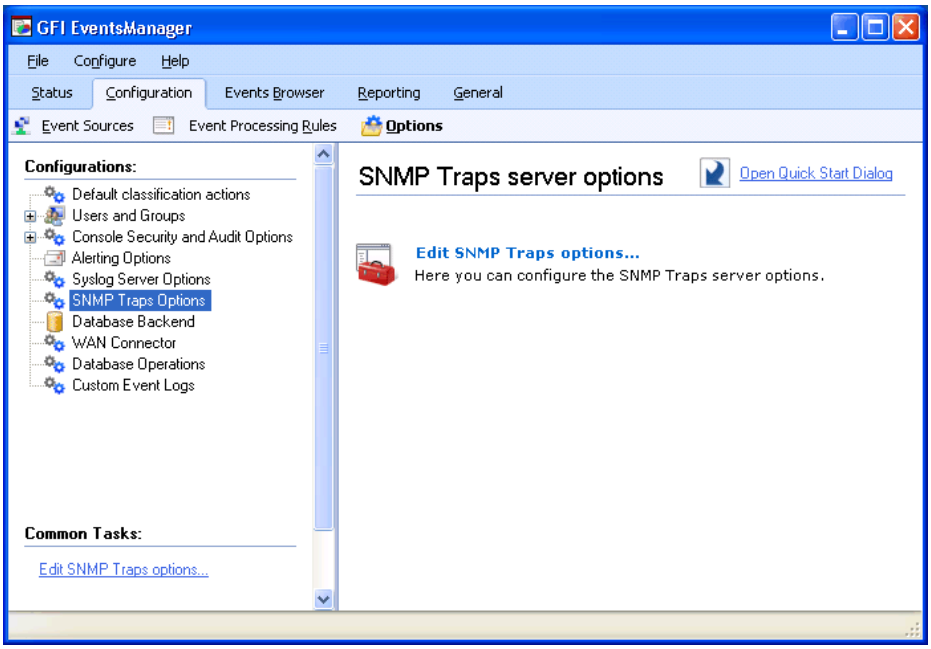
For information on how to archive events refer to the ‘Archiving events’ section in this chapter.

Selecting SNMP Trap processing rules

For information on how to select event processing rules refer to the ‘Selecting event processing rules’ section in this chapter.

7.8 Configuring the SNMP Trap server settings

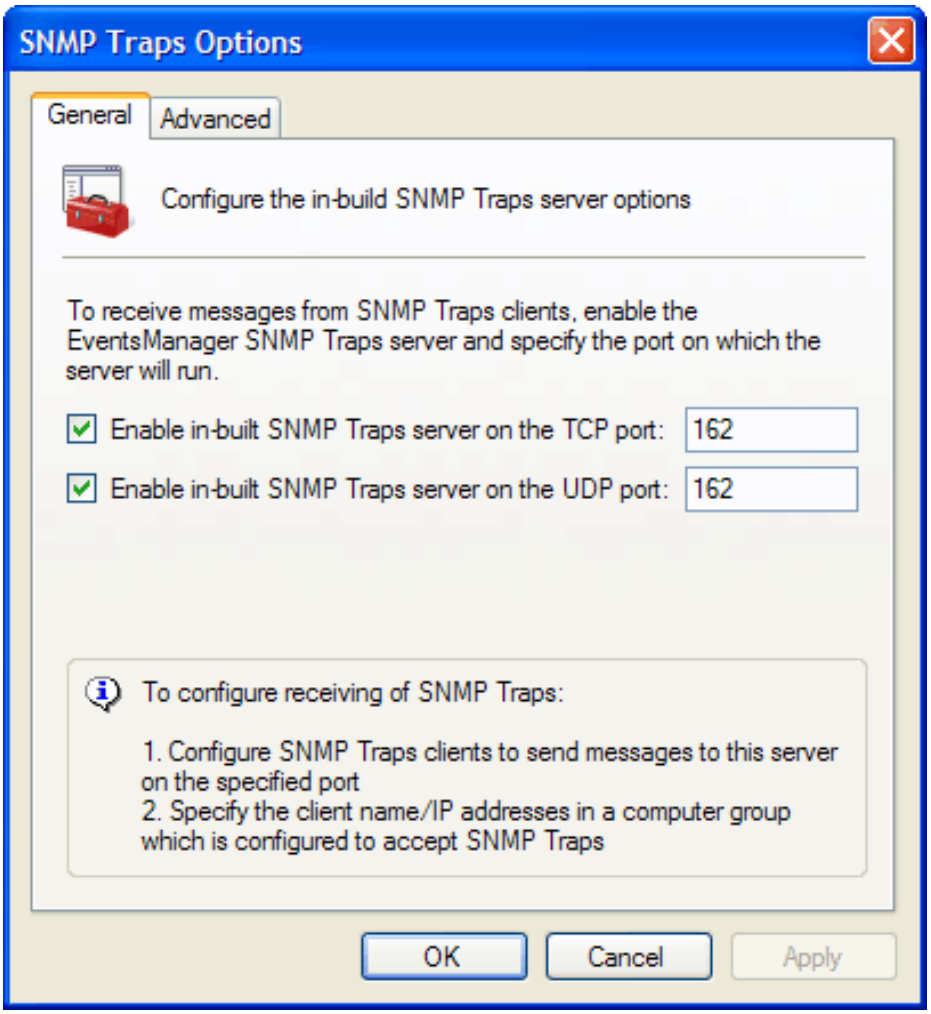
To change the default SNMP Trap Server settings:



Screenshot 65 - Configuring SNMP Traps

1. Click on the **Configuration** tab and select **Options**.

2. From the left pane, right-click the **SNMP Traps Options** node and select **Edit SNMP Traps options…**


SNMP Traps Options
General
Advanced
Configure the in-build SNMP Traps server options
To receive messages from SNMP Traps clients, enable the EventsManager SNMP Traps server and specify the port on which the server will run.
Enable in-built SNMP Traps server on the TCP port:
162
Enable in-built SNMP Traps server on the UDP port:
162
To configure receiving of SNMP Traps:
1. Configure SNMP Traps clients to send messages to this server on the specified port
2. Specify the client name/IP addresses in a computer group which is configured to accept SNMP Traps
OK
Cancel
Apply

Screenshot 66- SNMP Traps options

3. Enable the required TCP/UDP SNMP server. Specify the TCP/UDP port on which GFI EventsManager will listen for SNMP messages.

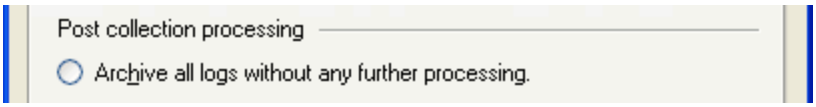
4. Click on the **Advanced** tab if you want to add, edit or remove SNMP Trap object identifiers (OIDs).

5. Click **OK** to finalize your configuration settings.

NOTE: When configuring SNMP Trap Server port settings, make sure that the configured TCP or UDP port is not already in use by other installed applications. This may affect the delivery of SNMP Trap messages to GFI EventsManager.

7.9 Archiving events

Archive events without processing logs



Screenshot 67 - Archiving events without processing

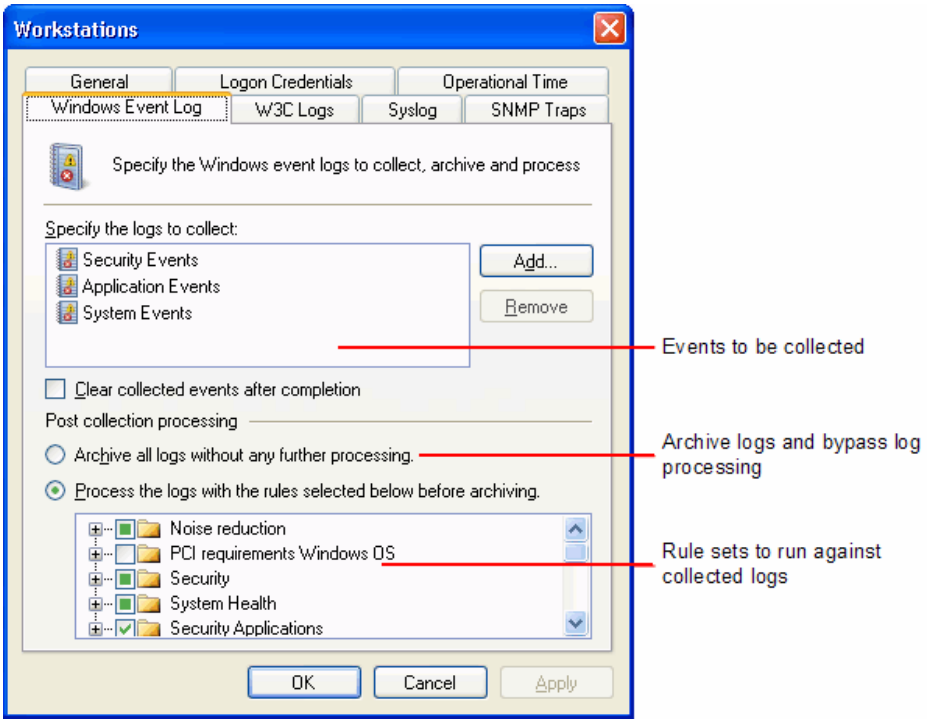
By default, GFI EventsManager is configured to process all event logs collected from target computers. To archive events without processing logs, select the 'Archive only' option.

Archiving events after processing

Processed events can be optionally archived into the GFI EventsManager database backend. By default, GFI EventsManager can be configured to automatically archive events:

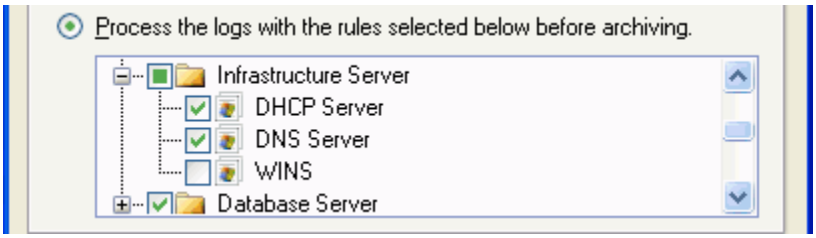
- Based on their classification. For example, you can configure default settings which archive only critical events. For information on how to configure event archiving based on event classification refer to the 'Configuring default classification actions' in the 'Configuring alerts and actions' chapter.
- Based on the conditions configured in the event processing rules. Rules provide an alternative and more flexible way to archive processed events. Through these rules, you can selectively archive only those events that satisfy specific rule condition(s) - regardless their classification. For example, you can configure a rule which archives only critical events with ID 537. For more information on how to create and configure event processing rules refer to the 'Configuring event processing rules' chapter.

7.10 Selecting event processing rules



Screenshot 68 - Computer group properties: Configuring Windows Event Logs parameters

In order to process and classify events, you must specify which rules will be applied against the collected logs. This is achieved by selecting the rule-sets folder or rule-set(s) that contain the required event processing rules.



Screenshot 69 - Selecting event processing rules/rule-sets

However, you must pay attention and choose the right “rule” for the job. The rule-sets that ship with GFI EventsManager are pre-configured to specific logs; therefore it is imperative that you choose rule-sets that can effectively process the events recorded in the collected logs.

Certain rule-sets contain specialized rules that are event specific. Therefore these rules will only be effective when used to process such specific events; failing to do so will result into erroneous event processing, data loss and non-significant results. For example, the ‘Monitoring and Attack detection’ rule-set contains rules specifically built to process Windows Security events. Therefore it will not be very effective if used to process Windows application events.

NOTE 1: By default, GFI EventsManager ships with pre-selected rules-sets/folders that can effectively process Windows Event Logs. If you are new to the product or you are not yet acquainted with the functionality of rule-sets, we recommend that you leave these settings as default.

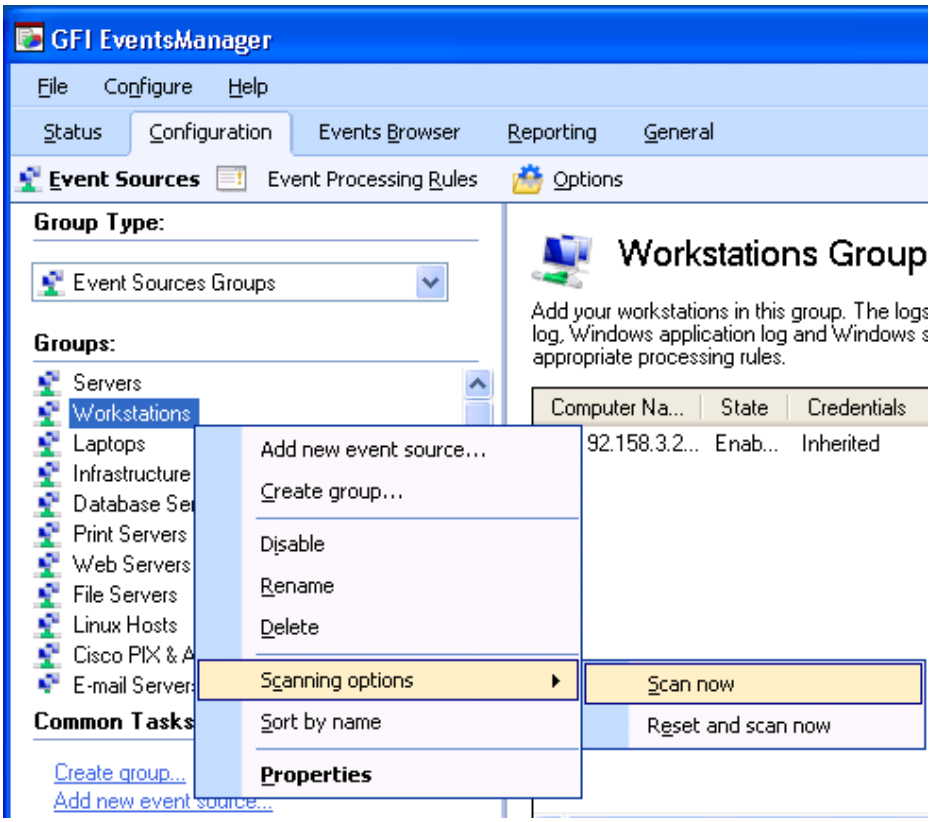
NOTE 2: If no rules-sets are shown in the selection window, this means that no event processing rules exist for the type of log being configured. For more information on how to configure event processing rules and rule-sets, refer to the ‘Configuring event processing rules’ chapter.

7.11 Triggering event source scanning manually

In GFI EventsManager, you can manually trigger an event collection iteration on target computers. To achieve this:

1. Right-click on the computer group which contains the required event sources.

2. Select **Scanning options > Scan now**.



Screenshot 70 - Triggering log collection manually

8 Customizing event processing rules

8.1 Introduction

Event processing rules are the conditions which:

- Classify processed events
- Filter out noise (repeated events) or unwanted events
- Trigger email, SMS and network alerts on key events
- Attempt remedial actions by executing specific scripts and executable files on key events.

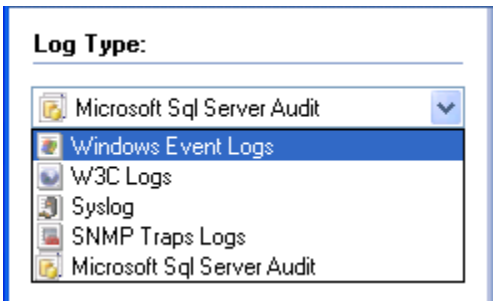
GFI EventsManager ships with pre-configured rules that can be used to process events with minor configuration effort. You can also customize these default rules or create tailored ones for all supported log types (i.e. Windows Event Logs, W3C, Syslog, SNMP Traps and SQL Server audit logs).

In GFI EventsManager, event processing rules are organized into rule-sets, which in turn are stored in rule-set folders. The pre-configured rules that ship with GFI EventsManager are organized into the following rule-set folders:

Rule-set folder	Description
Noise reduction rules	Contains rules tailored for the removal of repeated events and other noise from logs.
PCI requirements Windows OS	Contains rules tailored for PCI DSS compliance
Security	Contains rules tailored for the processing of Security logs and System logs.
System Health	Contains rules tailored for the processing of Application logs and System logs.
Security Applications	Contains rules tailored for the processing of Application logs, Security logs and System logs.
Infrastructure Server	Contains rules tailored for the processing of Application logs, DNS logs and System logs.
Database Server	Contains rules tailored for the processing of Application logs.
Web Server	Contains rules tailored for the processing of Application logs and System logs.
Print Server	Contains rules tailored for the processing of Application logs and System logs.
Terminal Services	Contains rules tailored for the processing of events generated terminal device driver services.
Email Server	Contains rules tailored for the processing of events generated by Microsoft Exchange server.
File Replication	Contains rules tailored for the processing of events generated by file replication services.

Directory Server	Contains rules tailored for the processing of events found in the Directory Services log.
HTTP protocol logs	Contains rules tailored for the processing of HTTP events logged by IIS Web Server(s)
FTP protocol logs	Contains rules tailored for the processing of FTP events logged by IIS Web server(s)
SMTP protocol logs	Contains rules tailored for to monitor events logged by ISS SMTP server(s).
Linux/Unix	Contains rules tailored for the processing of Syslogs.
Cisco PIX & ASA	Contains rules tailored for the processing of events generated by Cisco PIX firewalls and Cisco Adaptive Security Appliances

8.2 Create a new rule-set folder



Screenshot 71 - The log type drop-down list

To create a new rule-set folder:

1. Click on the **Configuration** tab and select **Event Processing Rules**.

2. From the provided drop-down, select the log-type for which you will be creating the rule-set folder.

3. Select the **Create folder** option from the 'Common tasks' area in the left pane.

4. Specify a unique name for the new rule-set folder.

8.3 Renaming and deleting folders

To rename or delete existing rule-set folders, right-click on the target rule-set folder and select **Rename** or **Delete** accordingly.

NOTE: Deleting a rule-set folder will lead to the deletion of all the rules and rule-sets contained within the deleted folder.

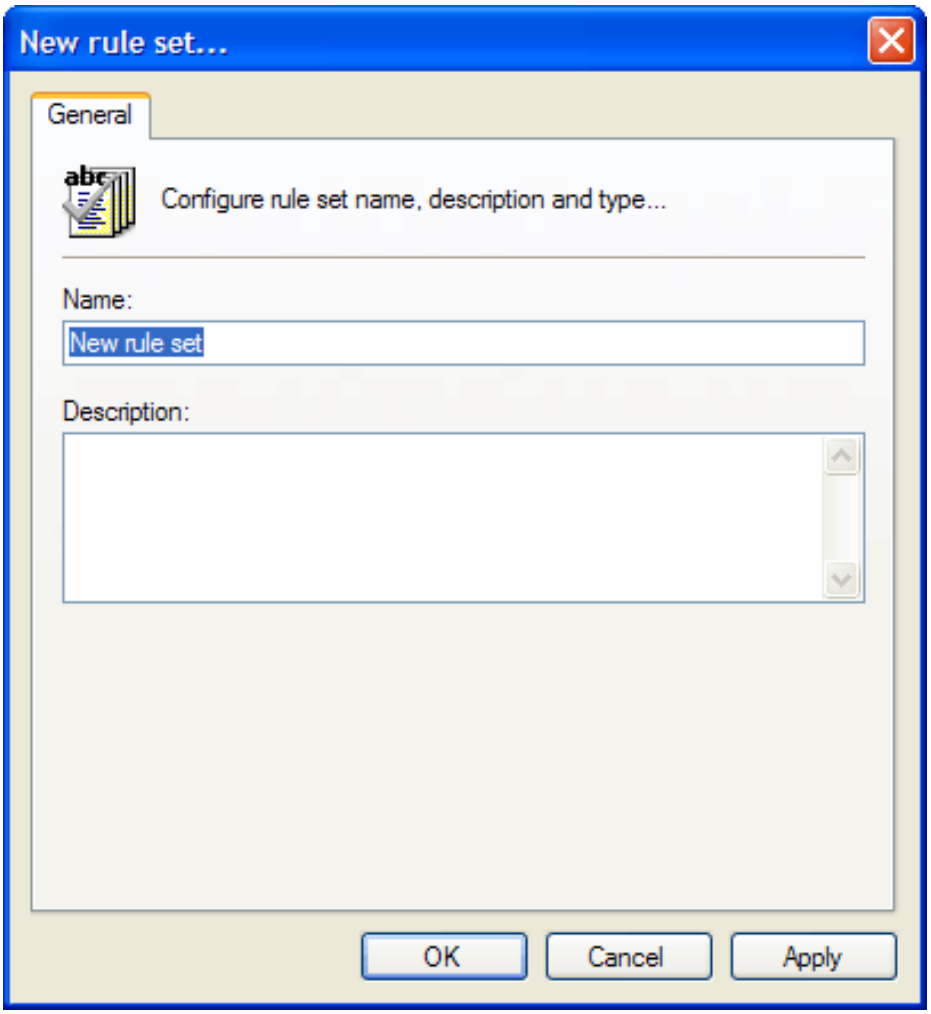
8.4 Creating a new rule-set

To create a new rule-set:

1. Click on the **Configuration** tab and select **Event Processing Rules**.

2. From the provided drop-down, select the log-type for which you will be creating the new rule-set.

3. Right-click on the folder where to create the new rule-set and select **Create new rule set…**



Screenshot 72 - New rule-set dialog box

4. Specify a name and a description for this new rule-set.
5. Click **OK** to finalize your settings.

8.5 Editing a rule-set

To edit rule-set parameters:

1. Right-click on the rule-set to edit and select **Properties**.
2. Make the required changes and click **OK** to finalize your settings.

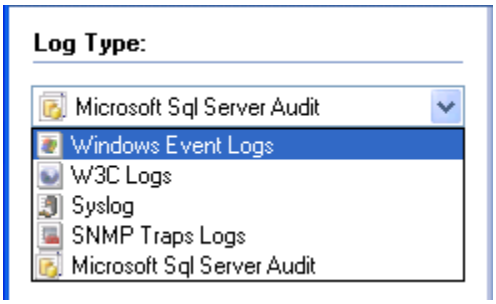
8.6 Deleting a rule-set

To delete a rule-set, right-click on the rule-set and select **Delete.**

8.7 Creating a new Windows Event Log rule

To create a new rule which is only applicable to Windows Event Logs:

1. Click on the **Configuration** tab and select **Event Processing Rules**.



Screenshot 73 - Selecting log-type from the provided drop-down

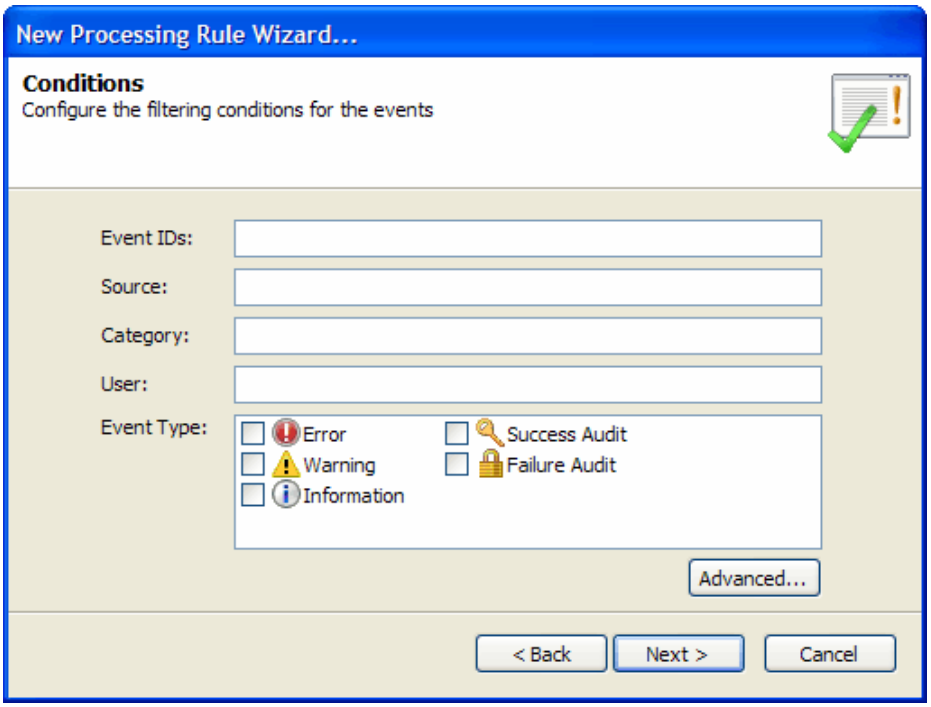
2. From the provided drop-down, select **Windows Event Logs**.

3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.

Screenshot 74 - GFI EventsManager: Select the Log(s)

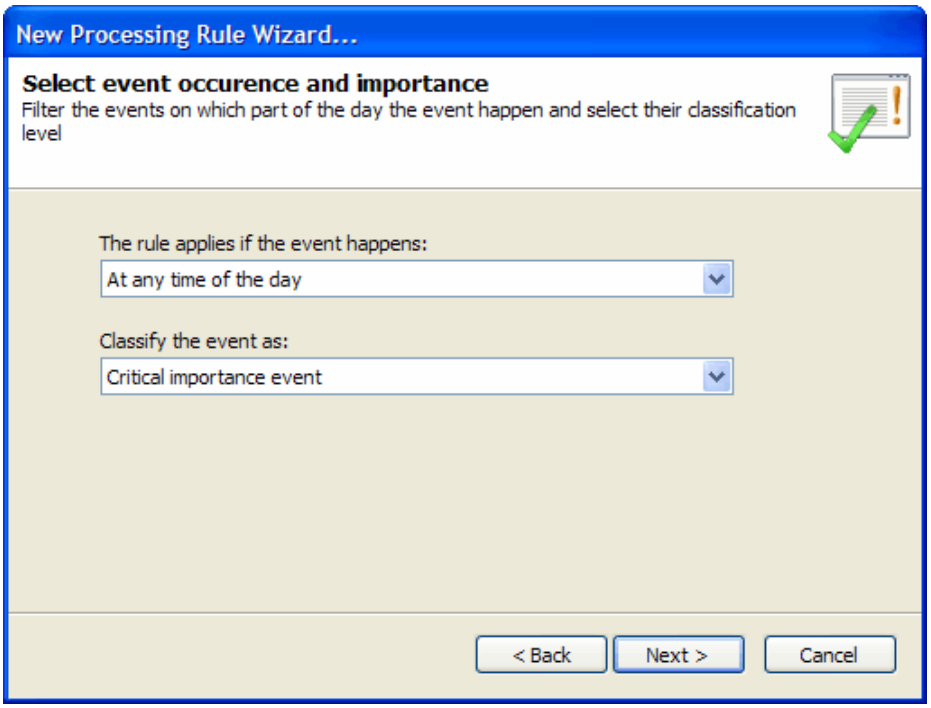
5. Select the event logs to which the rule applies and click **Next**.



Screenshot 75 - GFI EventsManager: Select the filtering conditions

6. Configure the event filtering conditions of this rule. To create a rule which will be applied to all events, leave the event ID empty. Click **Next** to continue.

NOTE: For more information on how to configure advanced event filtering conditions, refer to the 'Advanced event filtering parameters' section in this manual.

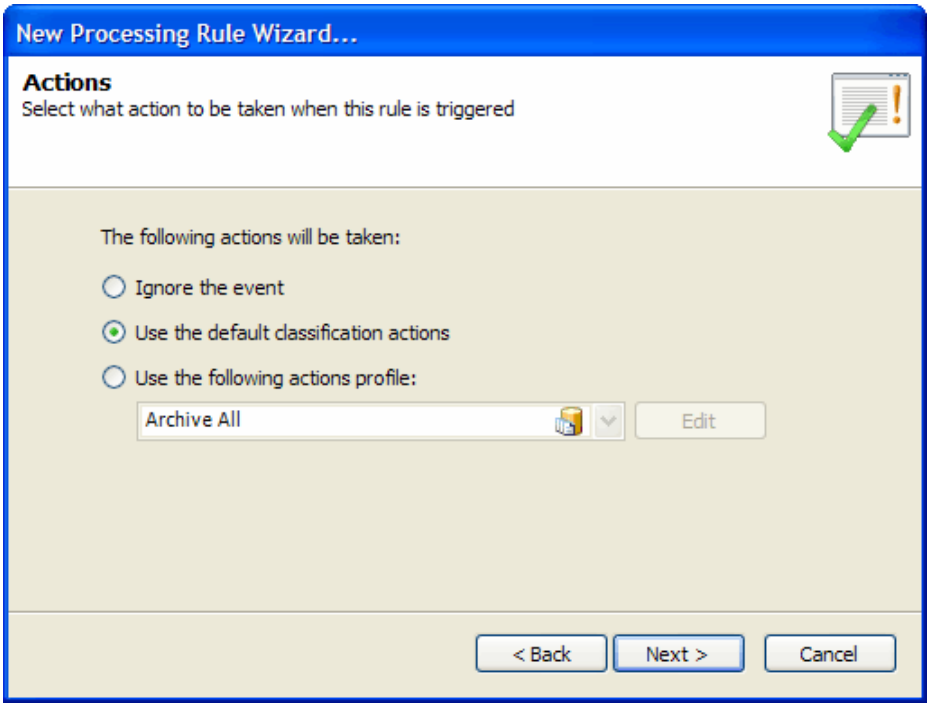

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 76 - New processing rule wizard: Select event occurrence and importance

7. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

NOTE: Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on how to configure operational times, refer to the 'Configuring event source operational time' section in the 'Configuring event sources' chapter.

8. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next** to continue.



Screenshot 77 - New processing rule wizard: Select action

9. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

10. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

NOTE: Newly created rules are disabled by default, hence will NOT become operational unless enabled. For information on how to enable event processing rules refer to the "Collecting and processing Windows events" section in this Manual.

8.8 Creating a new W3C rule

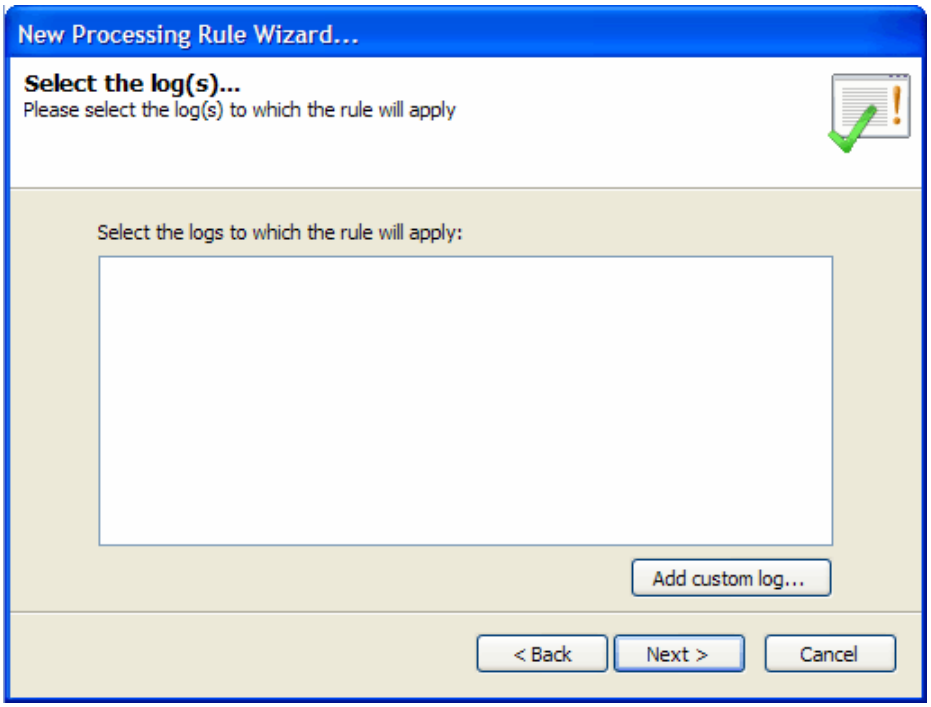
To create a new rule which is only applicable for W3C logs:

1. Click on the **Configuration** tab and select **Event Processing Rules**.

2. From the provided drop-down, select **W3C Logs**.

3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

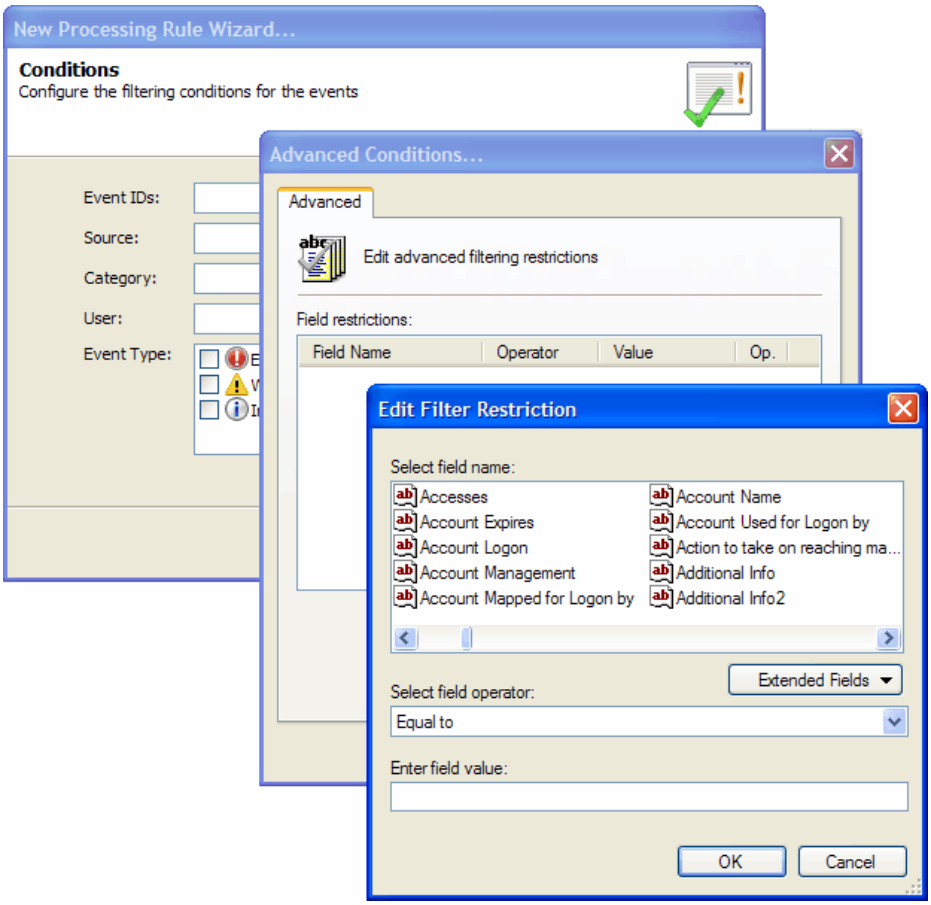
4. Specify a name and description for the new rule. Click **Next** to proceed with the configuration.


New Processing Rule Wizard...
Select the log(s)...
Please select the log(s) to which the rule will apply
Select the logs to which the rule will apply:
Add custom log...
< Back
Next >
Cancel

Screenshot 78 - New processing rule wizard: Select W3C Log

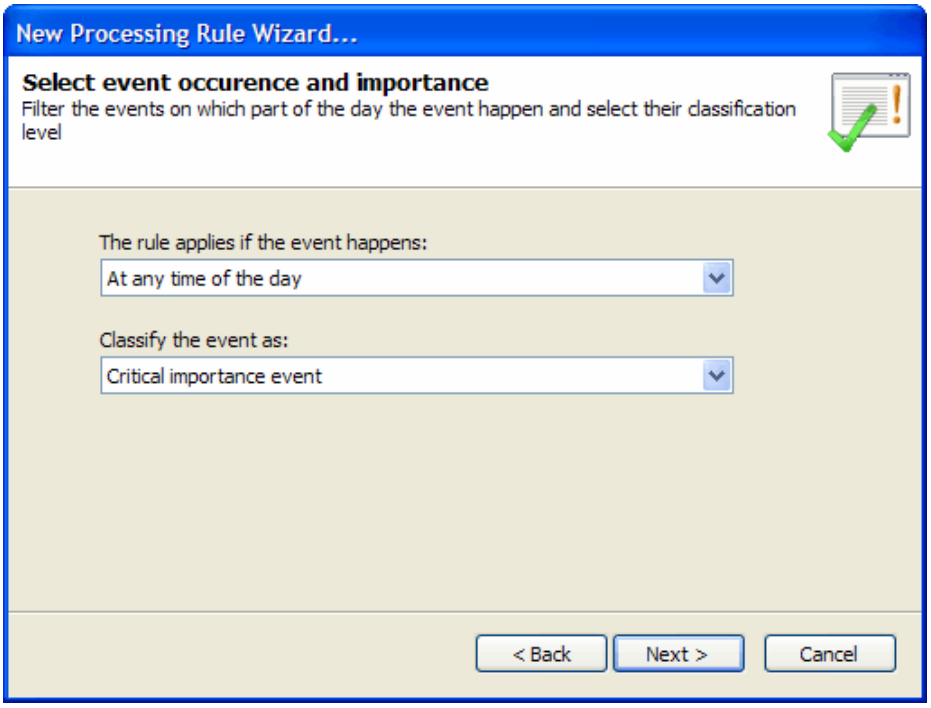
5. Click on the **Add** button. Specify the path to the W3C logs for which this rule applies or leave blank to apply this rule to all W3C logs. Click **Next** to continue.

NOTE: Multiple paths can be specified during configuration.



Screenshot 79 - New processing rule wizard: Configure filtering conditions.

6. Click on the **Add** button and configure event filtering conditions. Repeat until all conditions have been specified. Click **Next** to continue.

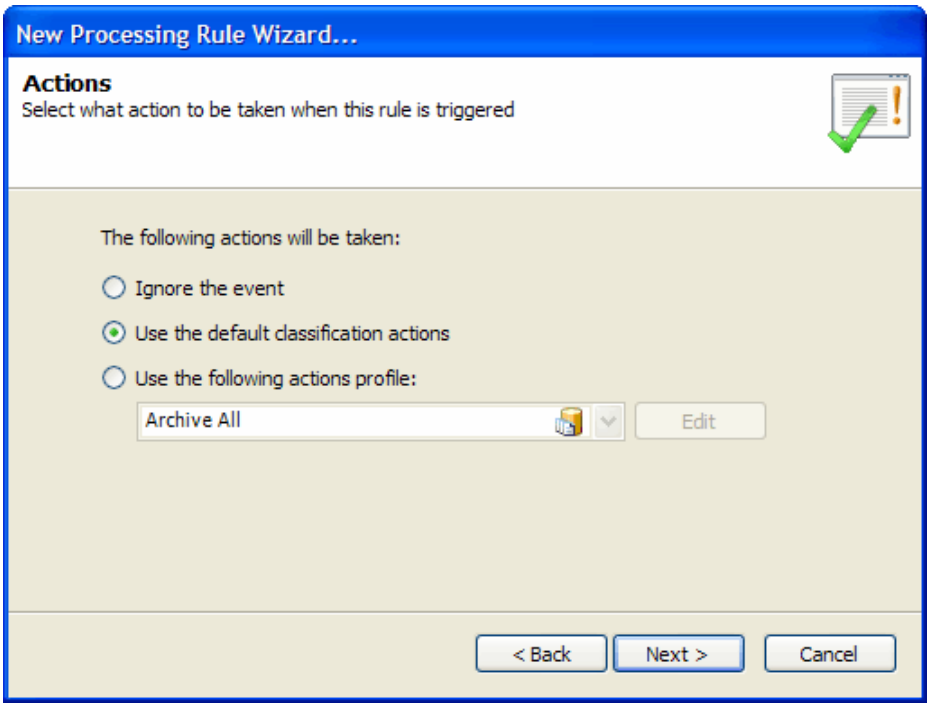

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 80 - New processing rule wizard: Select event occurrence and importance

7. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

NOTE: Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to the 'Configuring event source operational time' section in the 'Configuring event sources' chapter.

8. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next** to continue.



Screenshot 81 - New processing rule wizard: Select action

9. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

10. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

NOTE: Newly created rules are disabled by default, hence will NOT become operational unless enabled. For information on how to enable event processing rules refer to the “Collecting and processing W3C logs” section in this Manual.

8.9 Creating a new Syslog rule

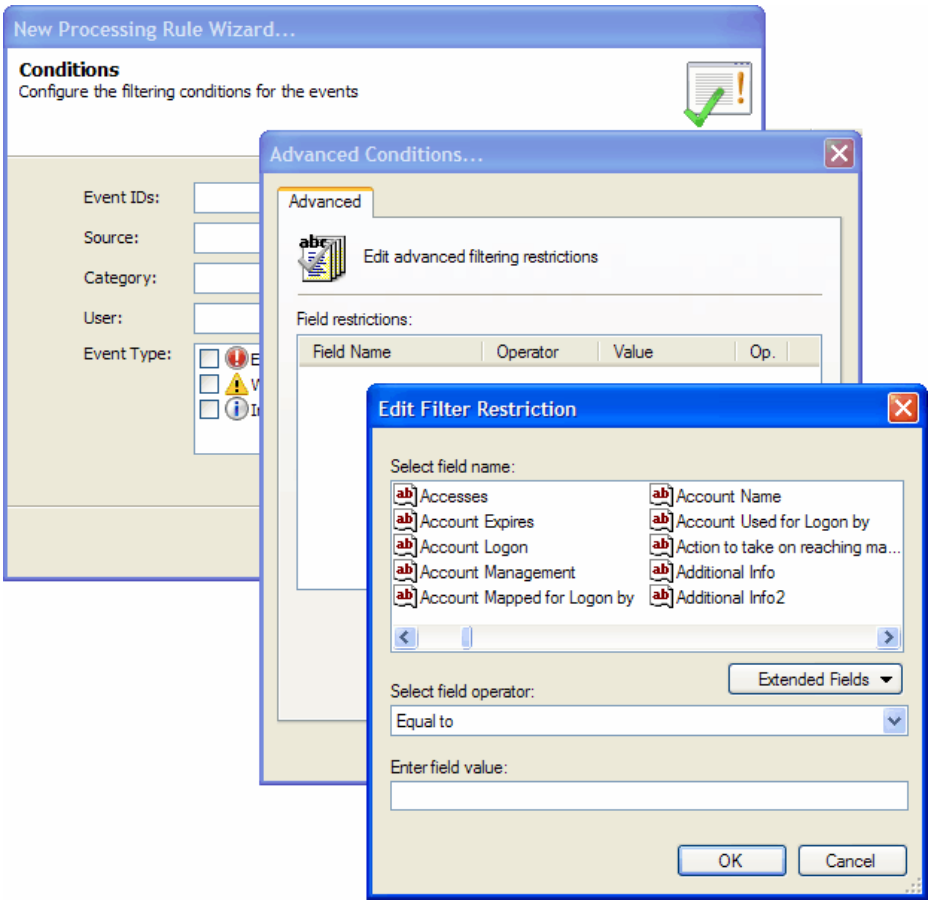
To create a new rule that is only applicable for the processing of Syslog messages:

1. Click on the **Configuration** tab and select **Event Processing Rules**.

2. From the provided drop-down, select **Syslog**.

3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

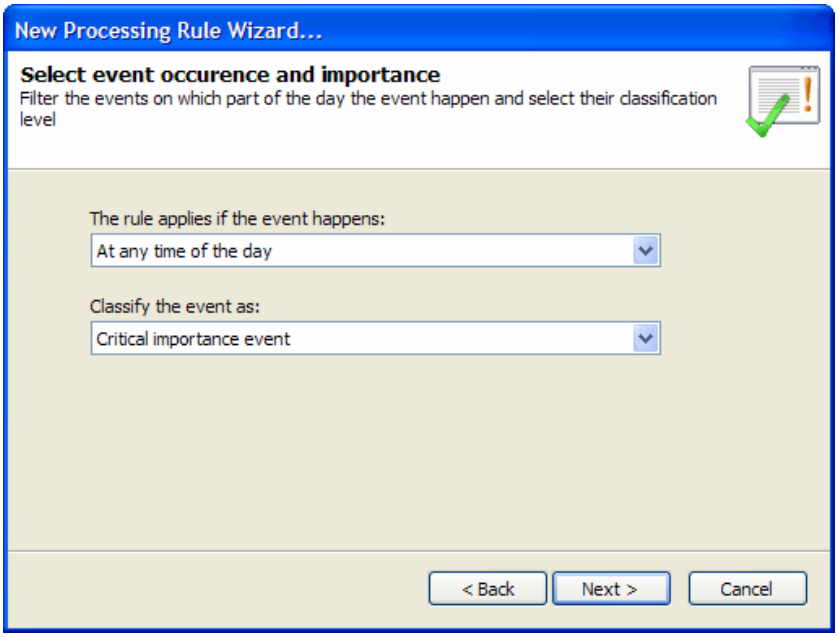
4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 82 - New processing rule wizard: Configure Conditions

5. Specify the log filtering conditions to be processed by this rule. When all conditions have been specified, click **Next**.

NOTE: For more information on how to configure advanced event filtering conditions, refer to the 'Advanced event filtering parameters' section in this manual.

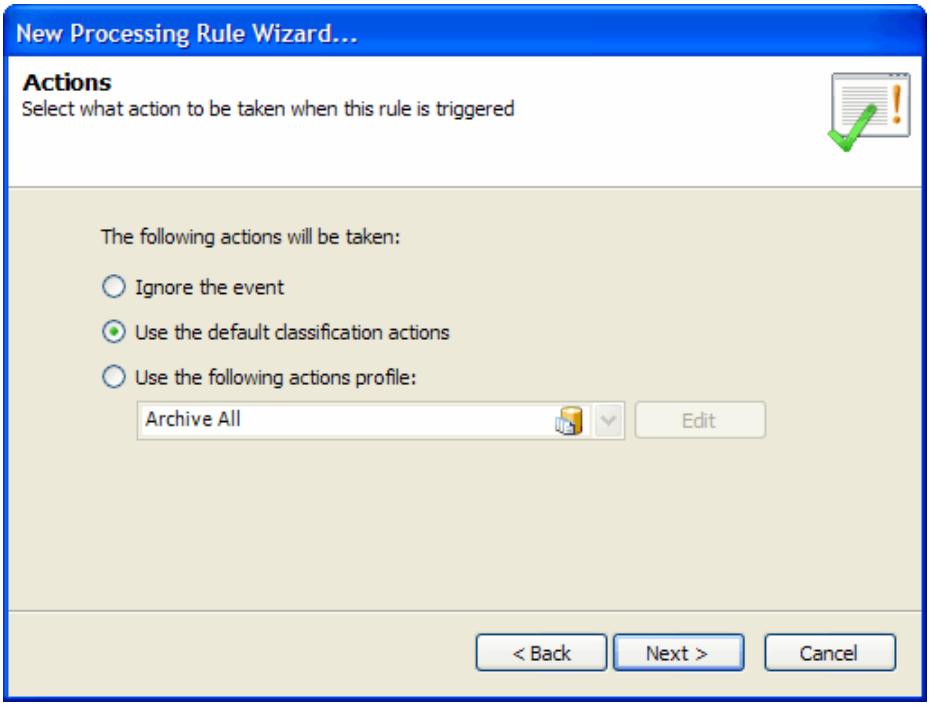

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 83 - New processing rule wizard: Select event occurrence and importance

6. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

NOTE: Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to the 'Configuring event source operational time' section in the 'Configuring event sources' chapter.

7. Select the classification (critical, high, medium, low) that will be assigned to events that satisfy this rule. Click **Next** to continue.



Screenshot 84 - New processing rule wizard: Select action

8. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

9. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

NOTE: Newly created rules are disabled by default, hence will NOT become operational unless enabled. For information on how to enable event processing rules refer to the "Collecting and processing Syslogs" section in this Manual.

8.10 Creating a new SNMP Trap rule

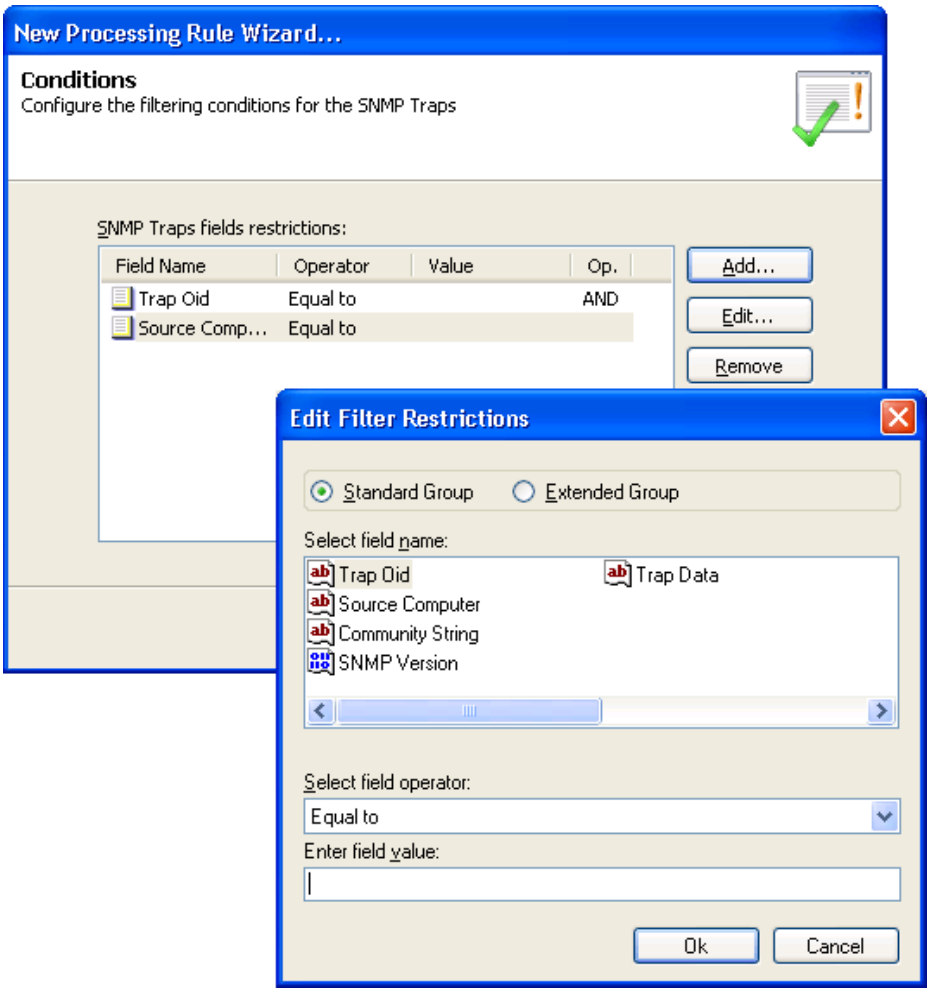
To create a new rule that is only applicable for the processing of SNMP Traps:

1. Click on the **Configuration** tab and select **Event Processing Rules**.

2. From the provided drop-down, select **SNMP Traps logs**.

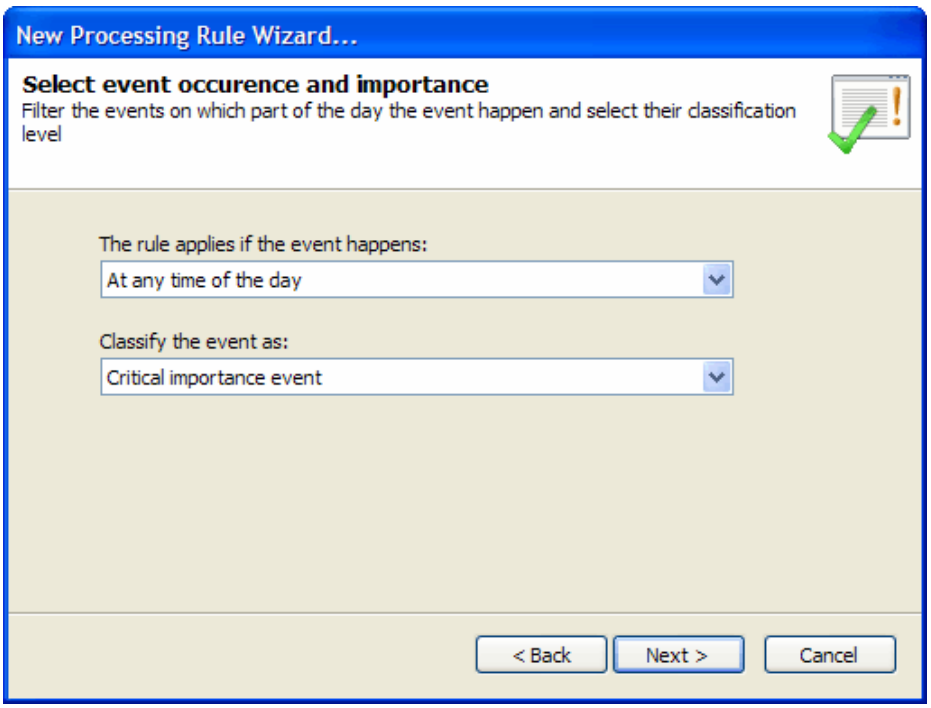
3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 85 - New processing rule wizard: Configure Conditions

5. Specify the log filtering conditions to be processed by this rule. When all conditions have been specified, click **Next**.

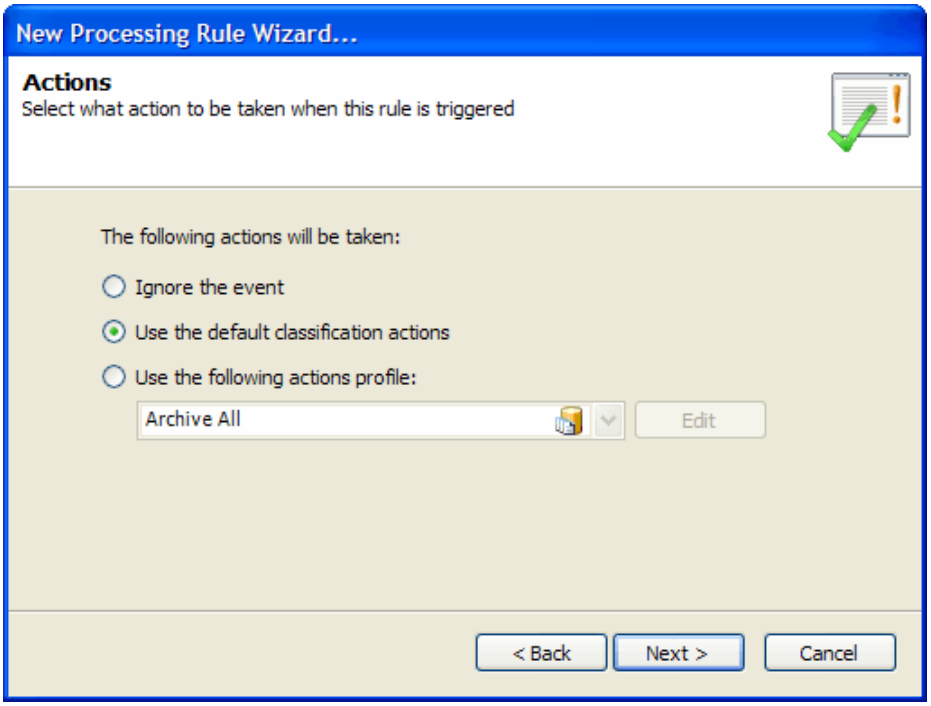

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 86 - New processing rule wizard: Select event occurrence and importance

6. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

NOTE: Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to the 'Configuring event source operational time' section in the 'Configuring event sources' chapter.

7. Select the classification (critical, high, medium, low) that will be assigned to events that satisfy this rule. Click **Next** to continue.



Screenshot 87 - New processing rule wizard: Select action

8. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

9. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

NOTE: Newly created rules are disabled by default, hence will NOT become operational unless enabled. For information on how to enable event processing rules refer to the "Collecting and processing SNMP Traps" section in this Manual.

8.11 Creating a new SQL Server audit log

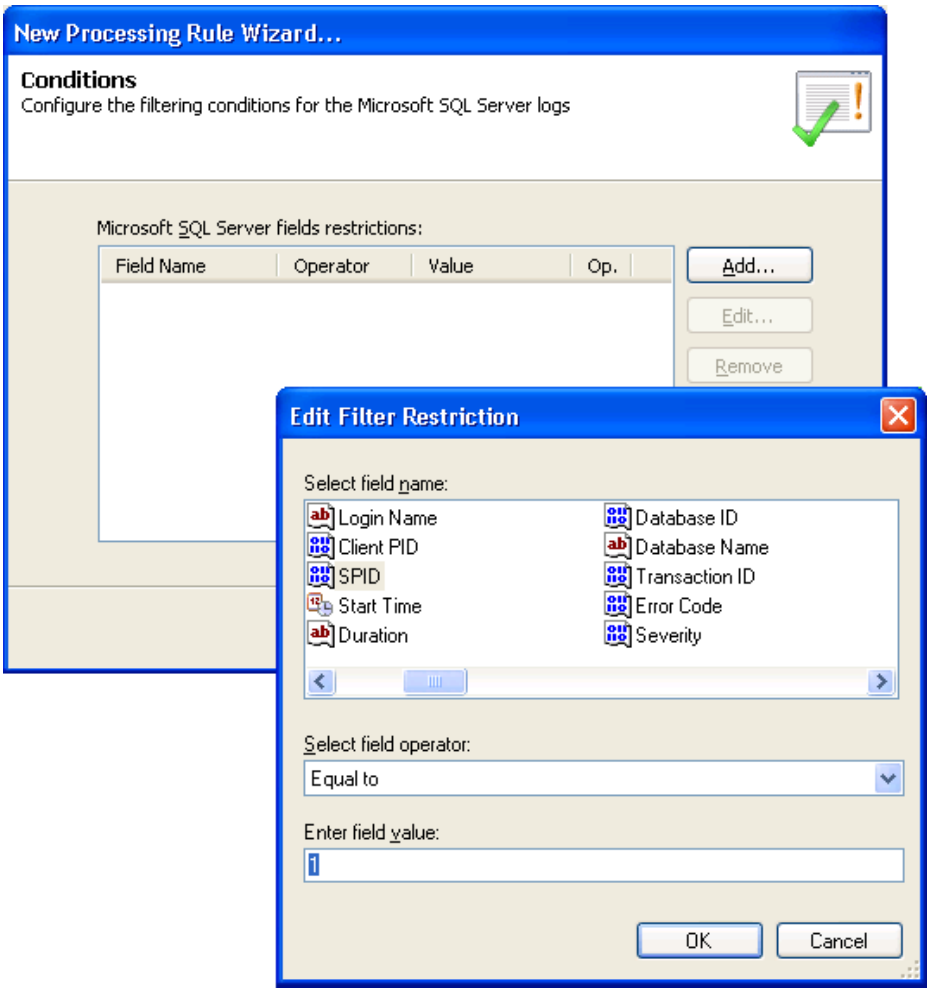
To create a new rule that is only applicable for the processing of SQL Server audit logs:

1. Click on the **Configuration** tab and select **Event Processing Rules**.

2. From the provided drop-down, select **Microsoft SQL Server audit**.

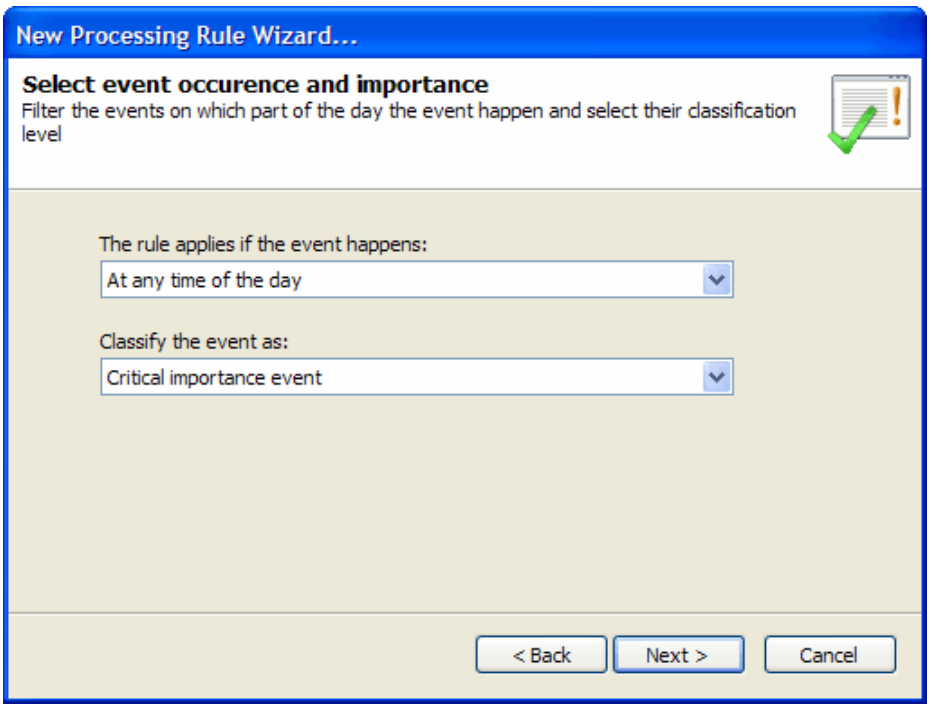
3. Right-click on the rule-set in which you will be creating the new rule and select **Create new rule…**

4. Specify the name and a description for the new rule. Click **Next** to proceed with the configuration.



Screenshot 88 - New processing rule wizard: Configure Conditions

5. Specify the log filtering conditions to be processed by this rule. When all conditions have been specified, click **Next**.

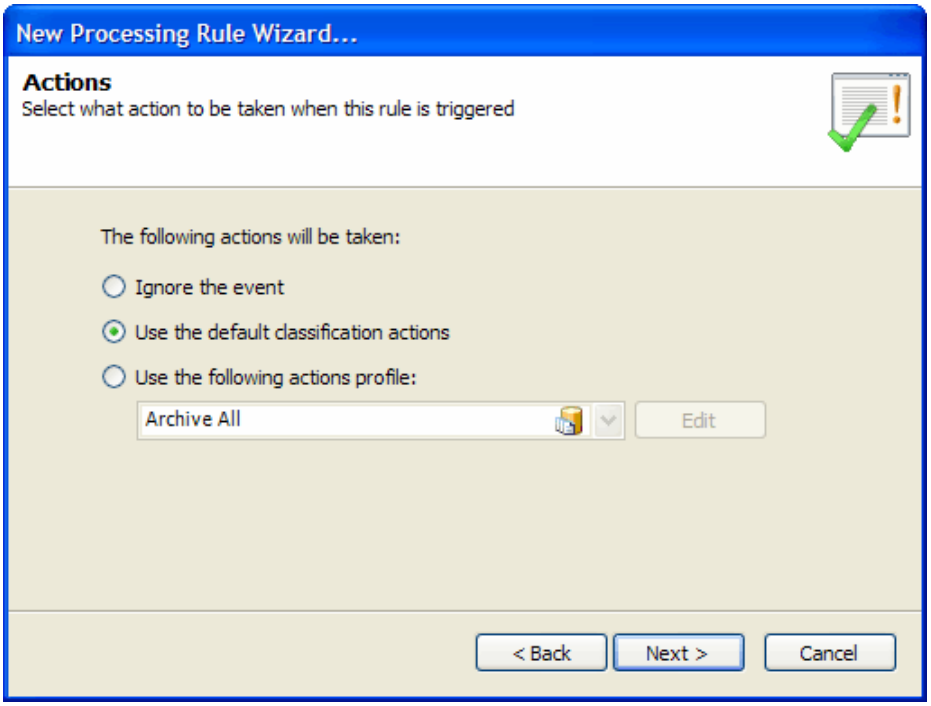

New Processing Rule Wizard...
Select event occurence and importance
Filter the events on which part of the day the event happen and select their classification level
The rule applies if the event happens:
At any time of the day
Classify the event as:
Critical importance event
< Back
Next >
Cancel

Screenshot 89 - New processing rule wizard: Select event occurrence and importance

6. Specify the time when this rule will be executed. (i.e. anytime, during working hours or outside working hours).

NOTE: Working and non-working hours are based on the operational time parameters configured for your event sources. For more information on operational times, refer to the 'Configuring event source operational time' section in the 'Configuring event sources' chapter.

7. Select the classification (critical, high, medium, low) that will be assigned to events that satisfy this rule. Click **Next** to continue.

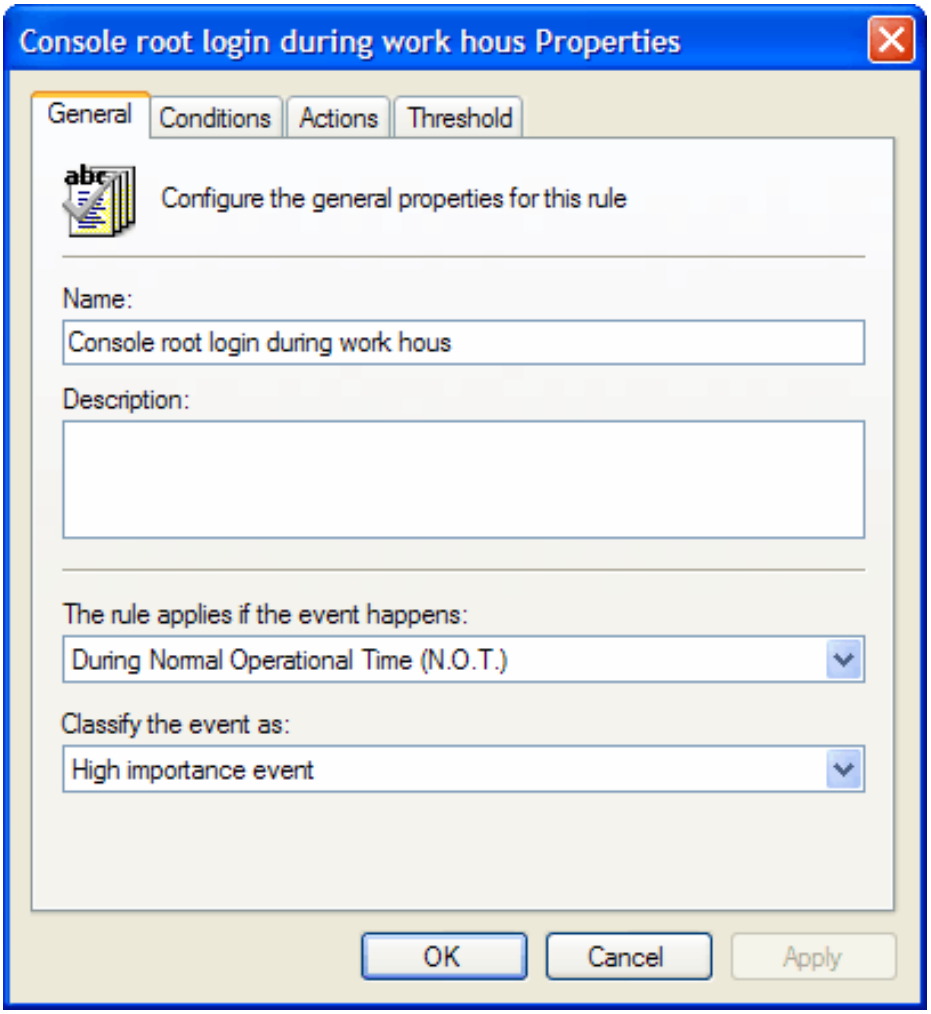


Screenshot 90 - New processing rule wizard: Select action

8. Specify which actions will be triggered by this rule. You can choose to ignore the event, trigger the default action, or customize alerts.

9. Click **Next** to proceed to the final dialog. Click **Finish** to finalize your settings.

8.12 Changing the configuration settings of a rule



Screenshot 91 - Log processing rule properties

To edit the property settings of an event processing rule:

1. Right-click on the rule and select **Properties**. This will bring up the 'Rule Properties' dialog.

2. Use the tabs provided in the dialog to navigate the existing parameters and make the required changes. The tabs provided in the properties dialog include:

- **General** - Use this tab to configure the general properties of the rule including the rule name and rule classification.
- **Logs** - This tab is available only for W3C log rules. Use this tab to specify the W3C logs for which this rule applies.
- **Event Logs** - This tab is available only for Windows Event Log rules only. Use this tab to specify which events will be processed by this rule.
- **Conditions** - Use this tab to configure event filtering conditions.
- **Actions** - Use this tab to configure alerts and actions triggered by this rule.
- **Threshold** - Use this tab to configure the event threshold value i.e. the number of times that an event must be detected prior to

triggering alerts and remedial actions. This helps reducing false positives triggered by noise (repeated events) in your event logs.

8.13 Advanced event filtering parameters

GFI EventsManager allows systems administrators to set up advanced event filtering parameters. These options are available only for Windows Events and Syslogs.

8.13.1 Windows events conditions

Event IDs field:

The 'Event IDs:' field allows systems administrators to setup:

Parameter type	Example
Single events	Event IDs: 575
List of events	Event IDs: 550, 570
Range of events	Event IDs: 575-600
Combination of events	Event IDs: 550, 570, 575-600

Source, category and user fields:

The 'Source', 'Category' and 'User' fields allow systems administrators to setup:

Parameter type	Example
Single source name	Source: Userenv
List of sources	Source: Userenv, SceCli
Wildcards (% and *)	Source: S%t%

8.13.2 Syslog categories

Message and process fields:

The 'Message' and 'Process' fields allow systems administrators to setup:

Parameter type	Example
Single message	Message: session opened
List of messages	Message: session opened, session closed
Wildcards (% and *)	Message: %session opened%

9 Customizing alerts and actions

9.1 Introduction

During event processing, GFI EventsManager can automatically generate various actions whenever particular events are encountered. Supported actions include email alerts and event archiving.

You can specify alerts and actions to be triggered in two ways:

1. By configuring a set of 'Default classification actions'.
2. By creating or customizing rules and rule-sets.

Default classification actions

Through the configuration parameters provided in the default classification actions, you can trigger alerts and actions based only on event classification. For example, default classification parameters can be configured to trigger email alerts for all classified events (critical, high, medium and low) but archive only critical events.

Generating actions through event processing rules

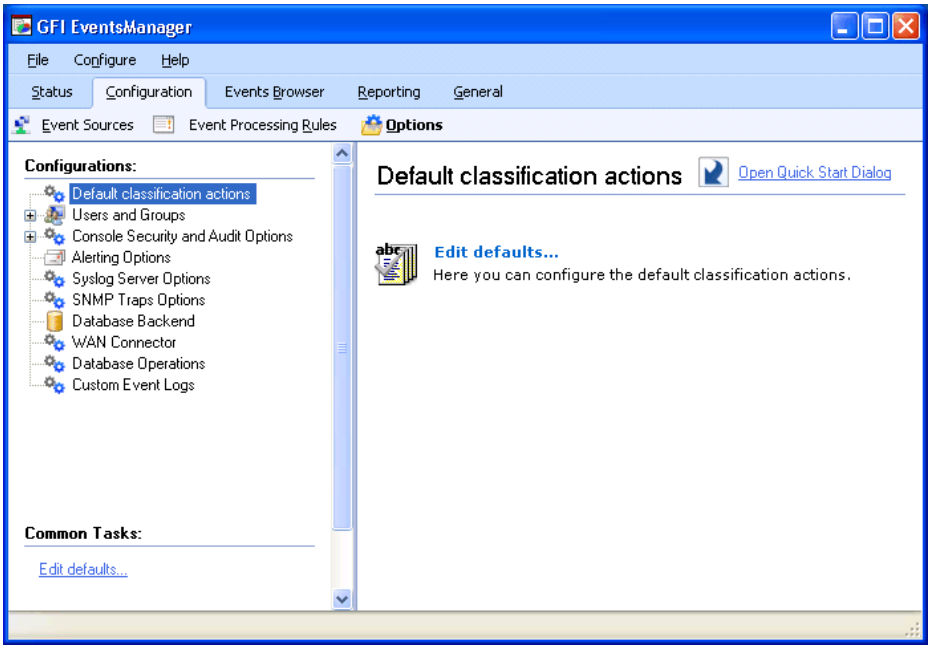
Rules allow you to configure actions on a more granular level. Rules allow you to configure and trigger actions whenever an event fits one or more specific conditions. For example, you can create a rule which archives only events having event ID 231, regardless their classification.

Supported actions

GFI EventsManager supports the following actions:

- **Archive the event** - Archives the classified event into the GFI EventsManager database back-end.
- **Send e-mail, SMS, network or SNMP notifications to** - Sends email, SMS network or SNMP alerts to specific recipients.
- **Run File** - Runs an executable file. Files that can be executed include VBScripts (.VBS), Batch files (.BAT) or another executable type of file (.EXE). You can also specify any command-line parameters to pass on to the executable file.

9.2 Configuring default classification actions

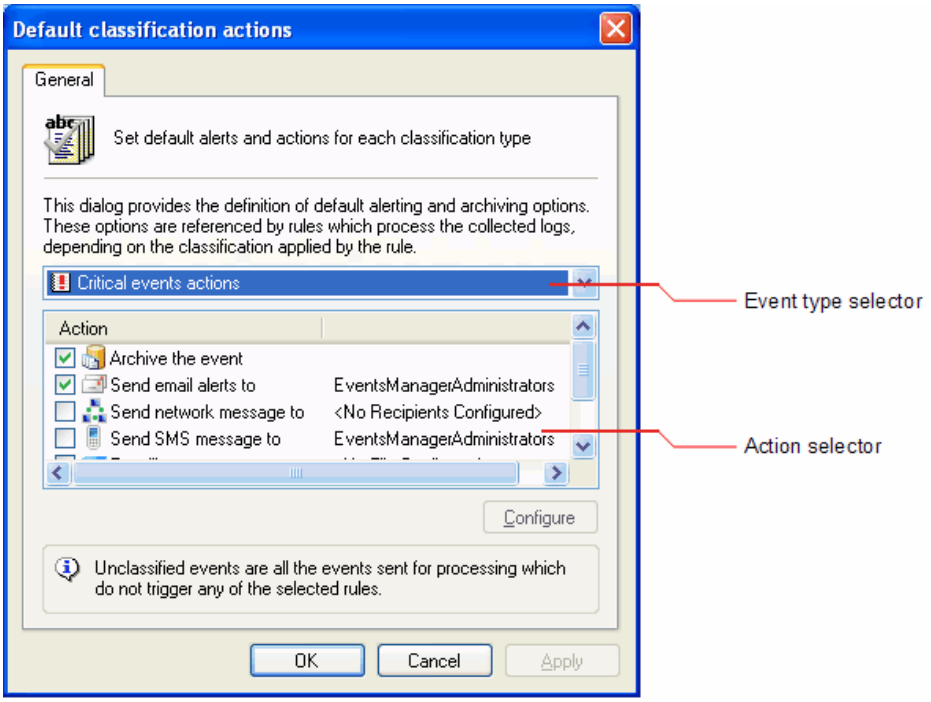


Screenshot 92 - Configuring default classification actions

To configure default classification actions:

1. Click the **Configuration** tab and select **Options**.

2. From the left pane, right-click on the **Default Classification Actions** node and select **Edit defaults…** option.


Default classification actions
General
Set default alerts and actions for each classification type
This dialog provides the definition of default alerting and archiving options. These options are referenced by rules which process the collected logs, depending on the classification applied by the rule.
Critical events actions
Event type selector
Action
Archive the event
Send email alerts to
EventsManagerAdministrators
Send network message to
<No Recipients Configured>
Send SMS message to
EventsManagerAdministrators
Action selector
Configure
Unclassified events are all the events sent for processing which do not trigger any of the selected rules.
OK
Cancel
Apply

Screenshot 93 - Default classification actions screen

3. From the provided drop-down, select the event classification to be configured.

4. From the provided list of supported actions, select the ones to be triggered for the selected classification.

5. Click on the **Configure** button specifies any parameters required by the selected action.

Be aware that assigning actions on events classified as low might generate:

- A lot of network traffic (especially if email, SMS, network or SNMP alerts are being generated)
- A high volume of database data/transactions if events are being archived.

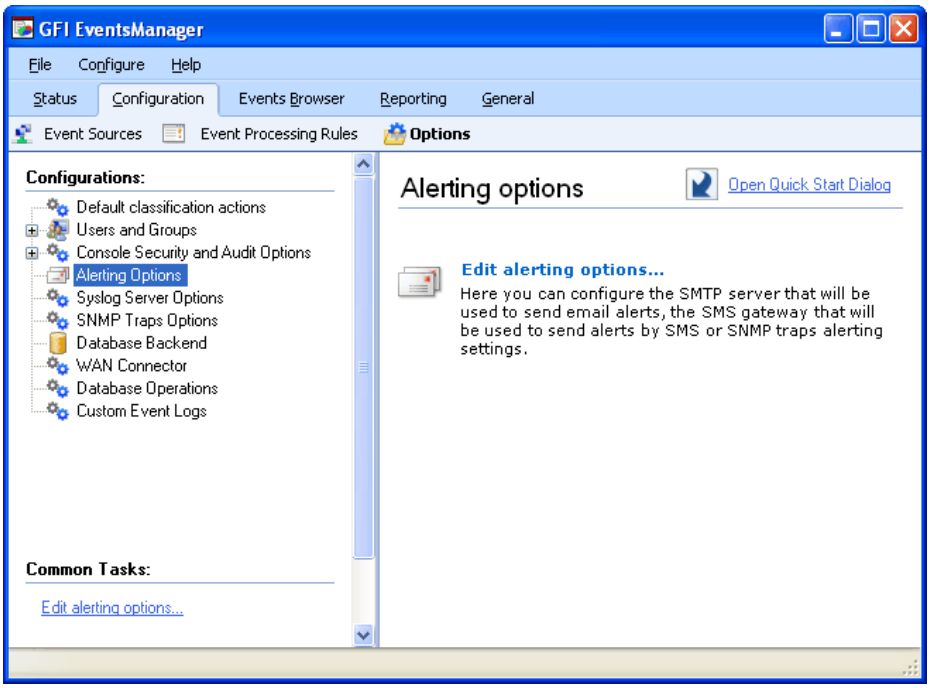
9.3 Configuring actions through event processing rules

For more information on how to trigger actions through event processing rules refer to the 'Configuring event processing rules' chapter.

9.4 Configuring alerting options

GFI EventsManager will automatically send out email, network, SMS or SNMP alerts whenever particular events are discovered. Supported alerting methods require the configuration of a set of general alerting parameters that are network specific. For example, to send email alerts, GFI EventsManager must know which SMTP Server will be used to propagate email alerts.

NOTE: While GFI EventsManager issues alerts automatically whenever particular alerts are discovered, it is important to configure the email address/es of the recipients of such alerts. By default, GFI EventsManager will automatically create the 'EventsManagerAdministrator' account to which you can assign an email address. For more information on how to configure administrator contact details refer to the 'Configuring the administrator account' section in the 'Configuring users and groups' chapter in this user manual.

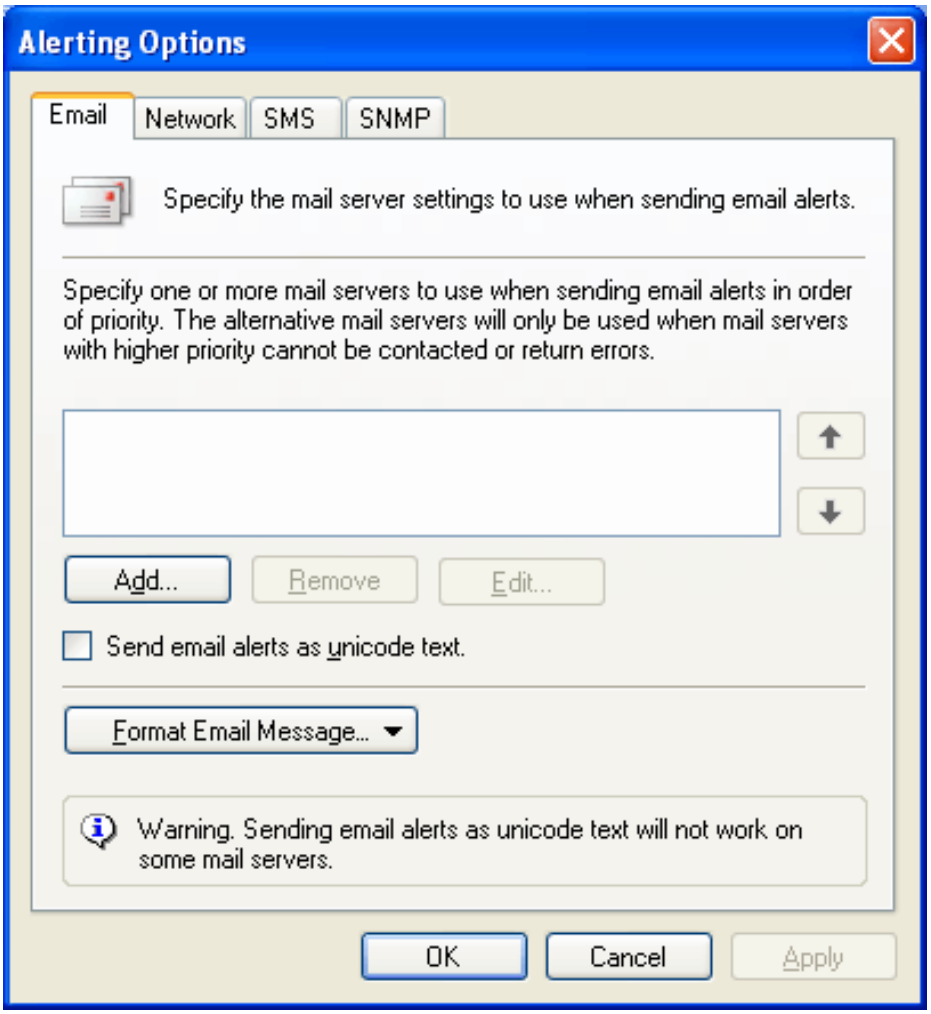


Screenshot 94 - Configuring alerting options

To configure alerts:

1. Click the **Configuration** tab and select **Options**.

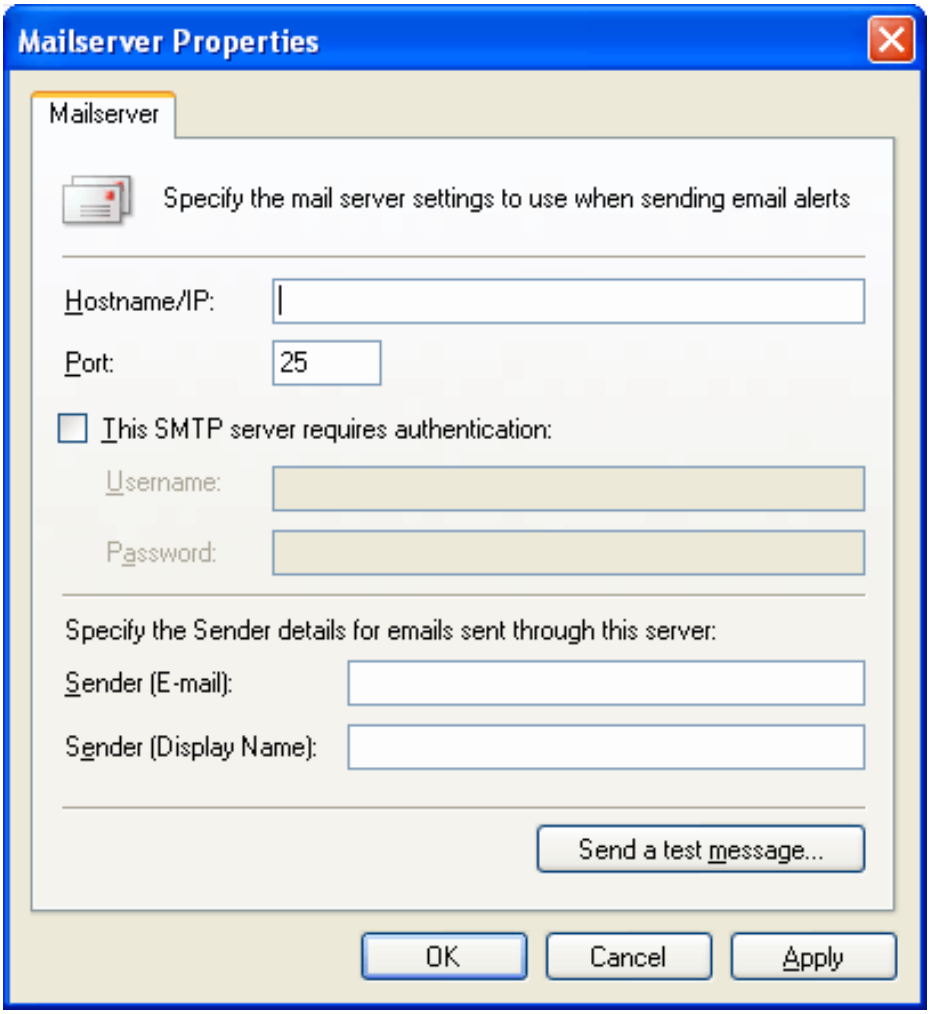
2. From the left pane, right-click on the **Alerting Options** node and select **Edit alerting options…** option.


Alerting Options
Email
Network
SMS
SNMP
Specify the mail server settings to use when sending email alerts.
Specify one or more mail servers to use when sending email alerts in order of priority. The alternative mail servers will only be used when mail servers with higher priority cannot be contacted or return errors.
Add...
Remove
Edit...
Send email alerts as unicode text.
Format Email Message...
Warning. Sending email alerts as unicode text will not work on some mail servers.
OK
Cancel
Apply

Screenshot 95 - Alerting options dialog

This will bring up the 'Alerting Options' dialog. Use the **Email**, **Network**, **SMS** and **SNMP** tabs provided in this dialog to configure the default alerting settings. More information on how to configure these settings is provided below.

9.4.1 Configuring email alerts



Screenshot 96- Mail server properties dialog box

To configure email alerts:

1. From the **Email** tab which opens by default, click on the **Add** button.

2. Specify the name/IP of your mail server. If required specify also the mail server authentication details.

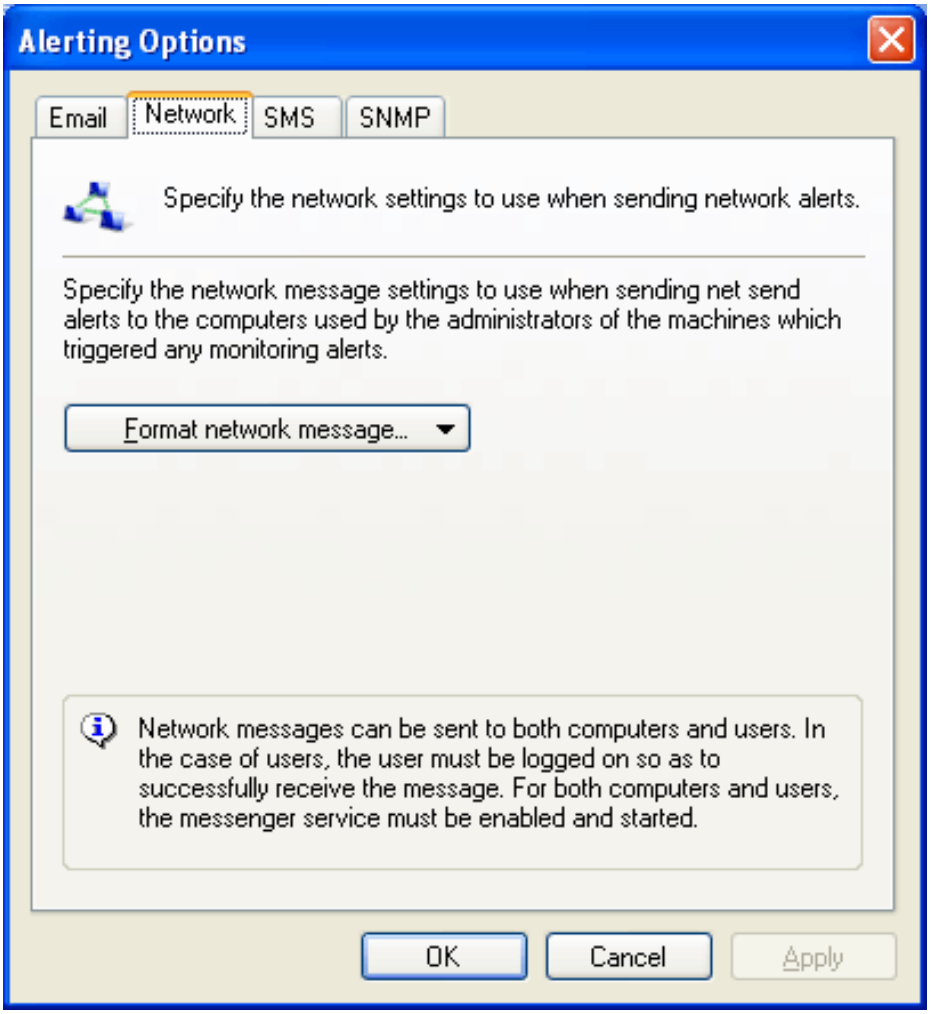
3. Specify the email address and display name that will be used when sending email alerts.

4. To customize the email text message, click on the **Format Email Message…** button.

5. If required, click on the **Network**, **SMS** or **SNMP** tabs to configure the respective parameters.

6. Click **OK** to finalize your settings.

9.4.2 Configuring network alerts

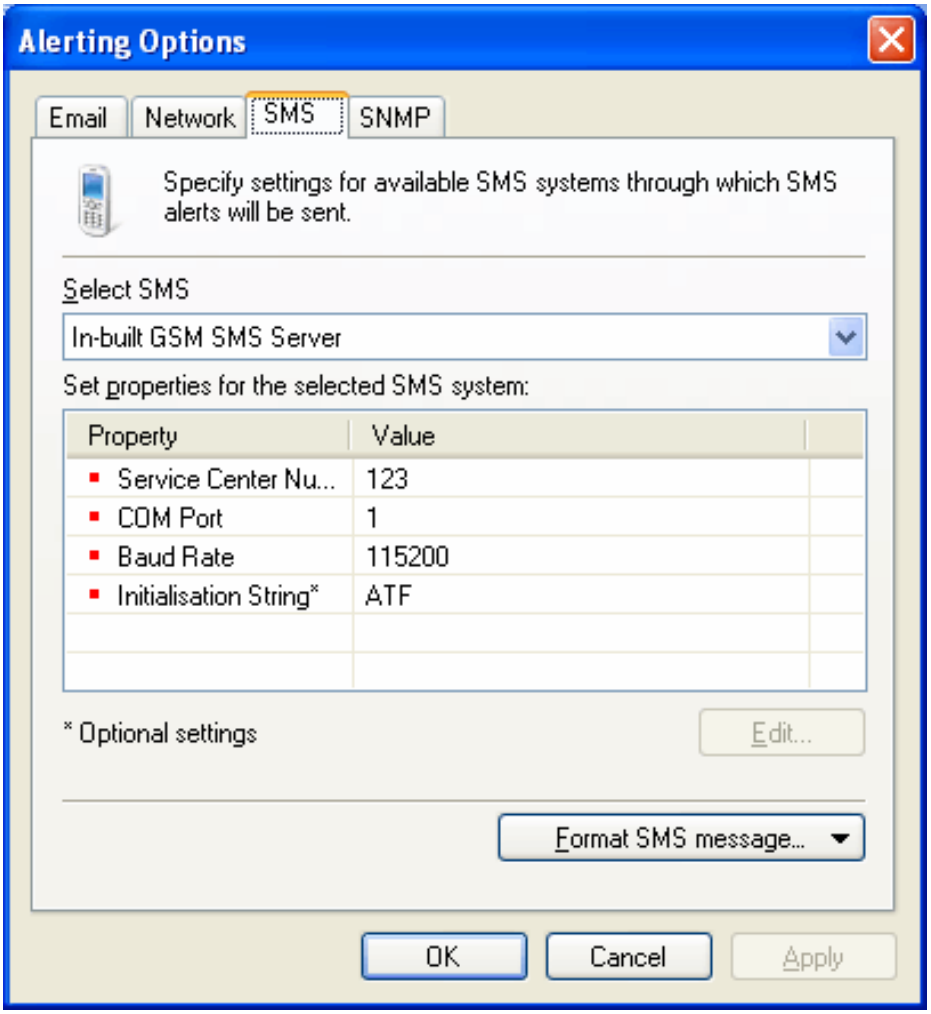

Alerting Options
Email
Network
SMS
SNMP
Specify the network settings to use when sending network alerts.
Specify the network message settings to use when sending net send alerts to the computers used by the administrators of the machines which triggered any monitoring alerts.
Format network message...
Network messages can be sent to both computers and users. In the case of users, the user must be logged on so as to successfully receive the message. For both computers and users, the messenger service must be enabled and started.
OK
Cancel
Apply

Screenshot 97 - Alerting Options: Network dialog box

1. Access the **Network** tab

2. No configuration settings are required for network alerts from this dialog. However, you can customize the network message by clicking on the **Format network message…** button.

9.4.3 Configuring SMS alerts



Screenshot 98 - Alerting Options: SMS dialog box

SMS alerts can be sent using various methods. Supported methods include GFI FAXmaker SMS gateway and Clickatell Email to SMS service gateway. To configure which method will be used to convey SMS alerts:

1. Access the **SMS** tab

2. From the provided drop-down, select the SMS system through which SMS notification will be sent.

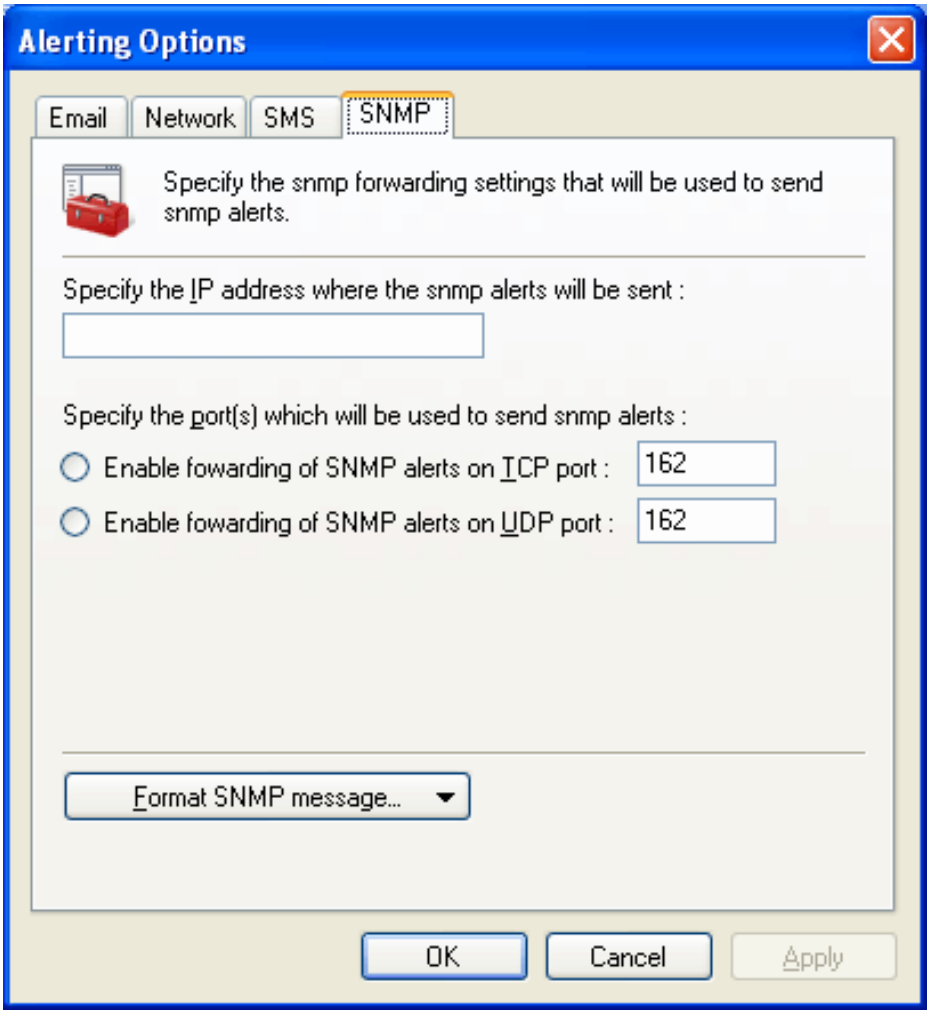
3. Select the property to be configured from the list provided and click **Edit…**

4. Repeat until all required properties have been configured.

5. To customize the SMS alert message, click on the **Format SMS message…** button.

6. Click on **OK** to finalize your settings.

9.4.4 Configuring SNMP alerts


Alerting Options
Email
Network
SMS
SNMP
Specify the snmp forwarding settings that will be used to send snmp alerts.
Specify the IP address where the snmp alerts will be sent :
Specify the port(s) which will be used to send snmp alerts :
Enable fowarding of SNMP alerts on TCP port :
162
Enable fowarding of SNMP alerts on UDP port :
162
Format SNMP message...
OK
Cancel
Apply

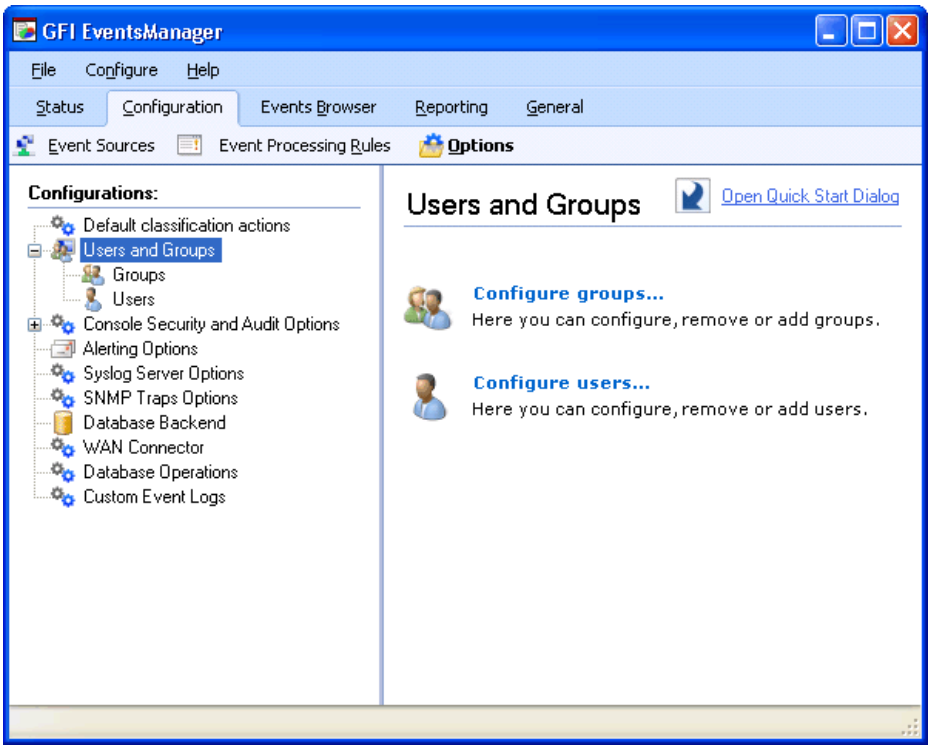
Screenshot 99 - Alerting Options: SNMP dialog box

To configure SNMP alerts:

1. Access the **SNMP** tab
2. Specify the IP address where SNMP alerts will be sent.
3. Optionally specify the port/s that will be used to send the SNMP alerts.
4. To customize the email text message, click on the **Format SNMP Message…** button.
5. Click **OK** to finalize your settings.

10 Configuring users and groups

10.1 Introduction



Screenshot 100 - Configuring users and groups node

Use the Users and Groups node to assign different console access privileges to GFI EventsManager users. Through this node users and groups can be configured, amended or deleted. Working hours and alerts can also be configured and assigned to groups.

Use the users and groups node also to assign users administrative privileges. These privileges allow users to browse events as well as modify GFI EventsManager configuration settings.

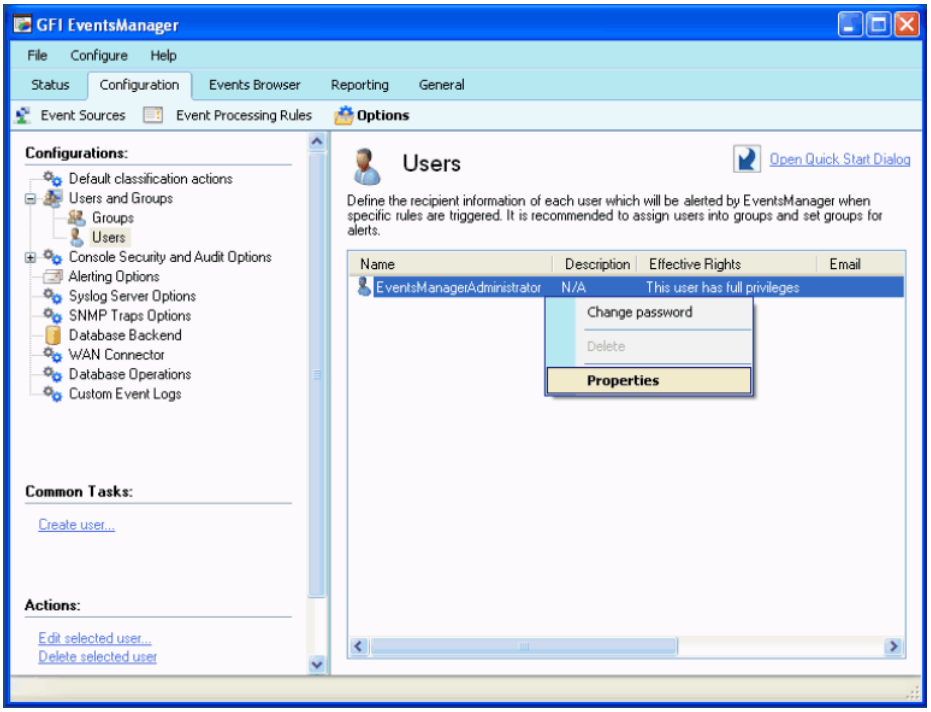
10.2 Configuring the administrator account

GFI EventsManager will automatically create the 'EventsManagerAdministrator' account. However, you must still configure details such as the email address and mobile number of the GFI EventsManager administrator.

NOTE: GFI EventsManager requires a valid administrator email address in order to distribute automatic alerts when particular events are discovered.

For every user (including the administrator), you can configure the following parameters:

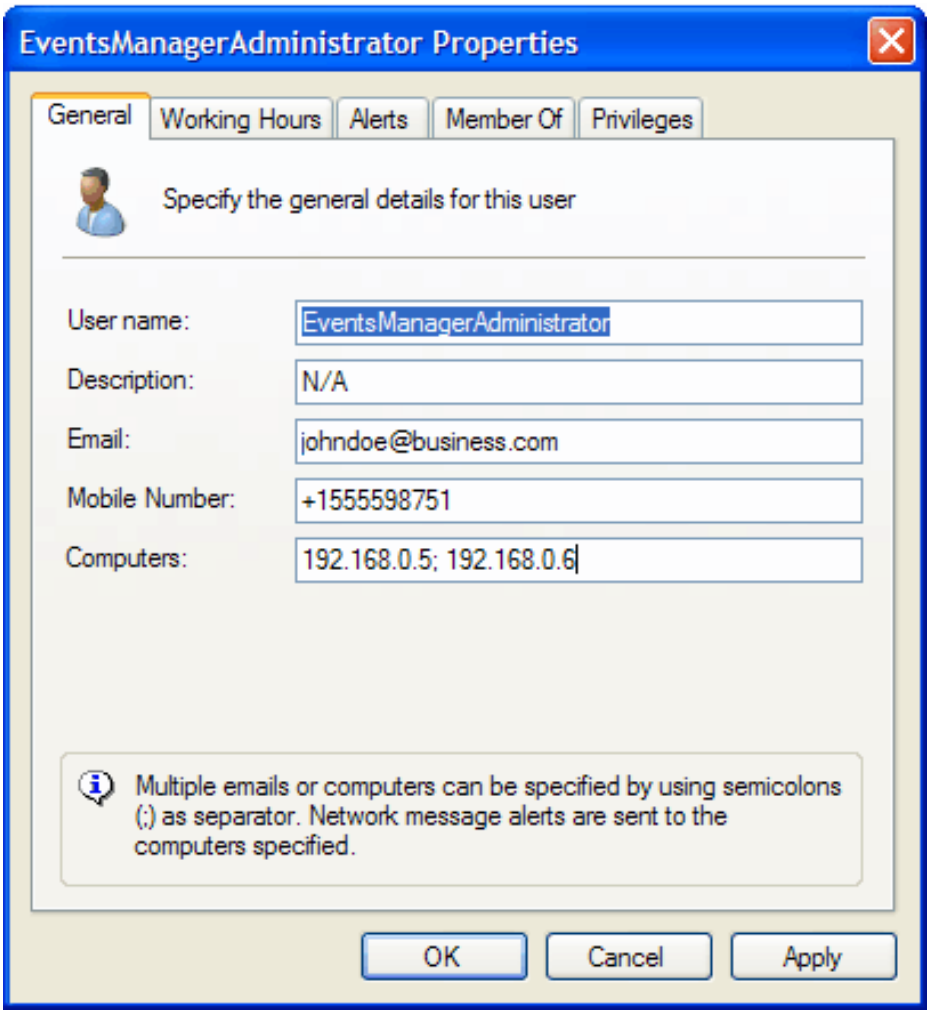
- Contact details including email address and phone number
- The typical working hours
- The type of alert to send during and outside working hours
- The notification group to which the user belongs.



Screenshot 101 - Configuring the default EventsManagerAdministrator account

To configure the GFI EventsManagerAdministrator account:

1. Click on the **Configuration** tab and select **Options**.
2. Expand the **Users and Groups** node.
3. Click on the **Users** sub-node and in the right pane right click on the **EventsManagerAdministrator** account and select **Properties**.



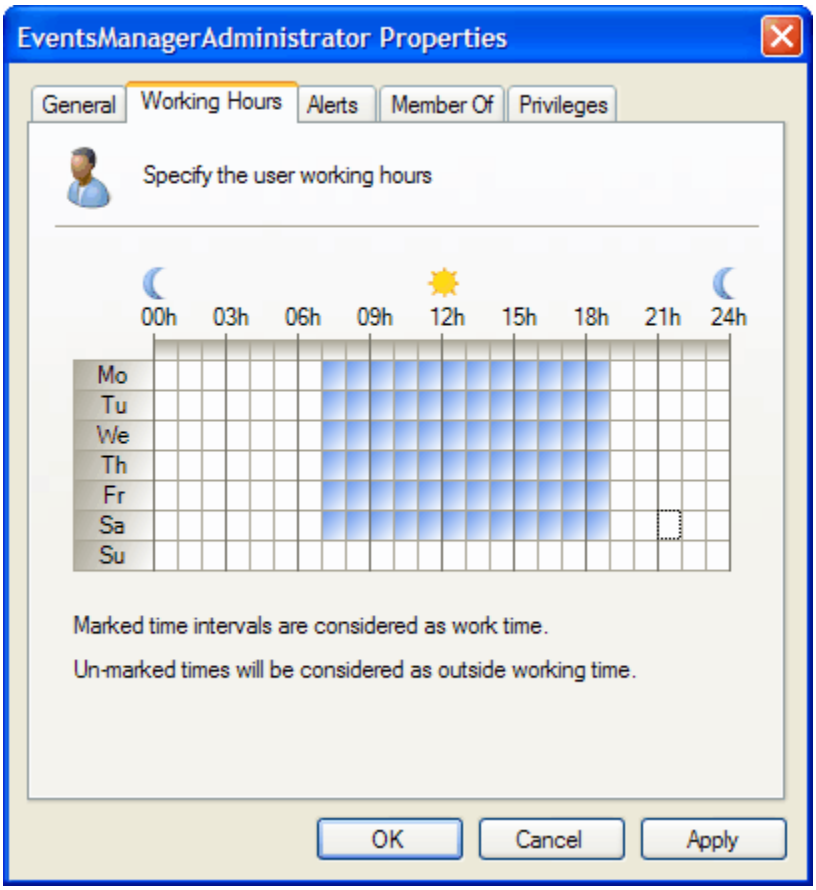
Screenshot 102 - EventsManager Administrator properties

This will bring up the 'EventsManagerAdministrator properties' dialog. Start configuring the account as follows:

1. Specify the contact details such as email address, and mobile number as required.

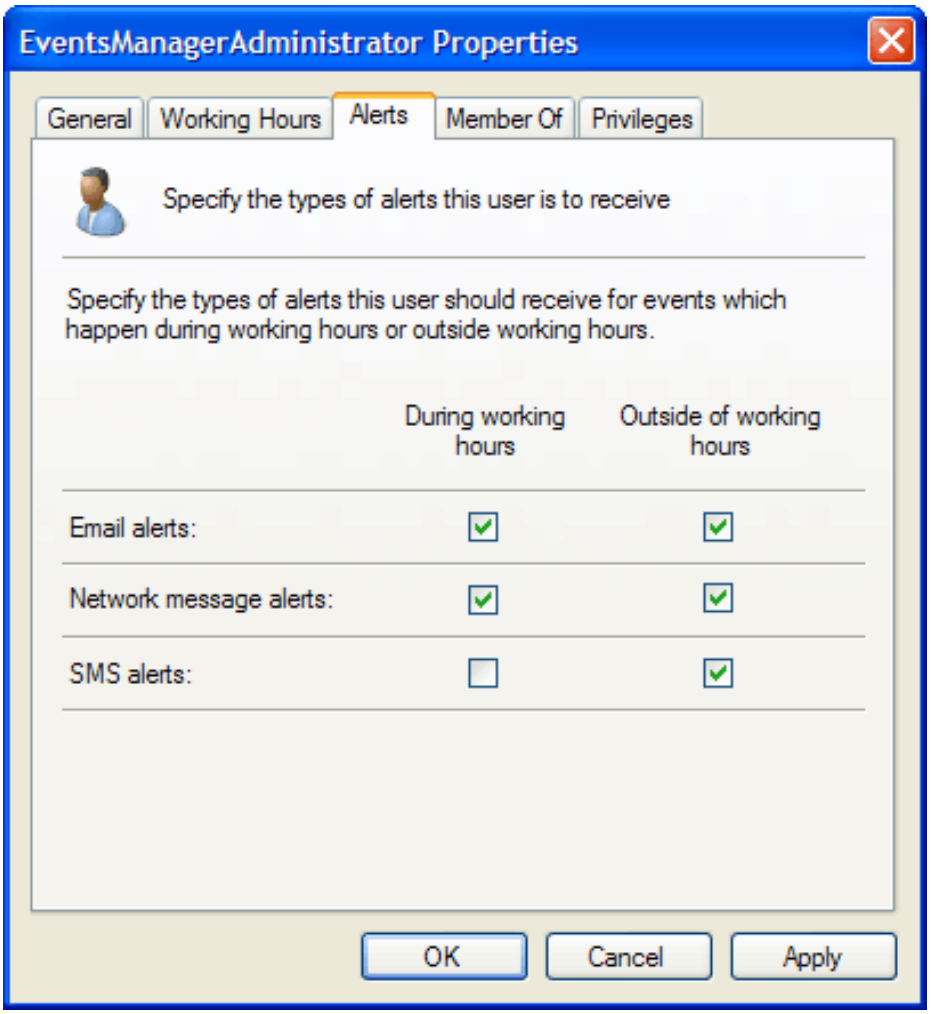
2. Specify the computers on which network alerts addressed to the administrator will be sent.

3. Click on the **Working Hours** tab.



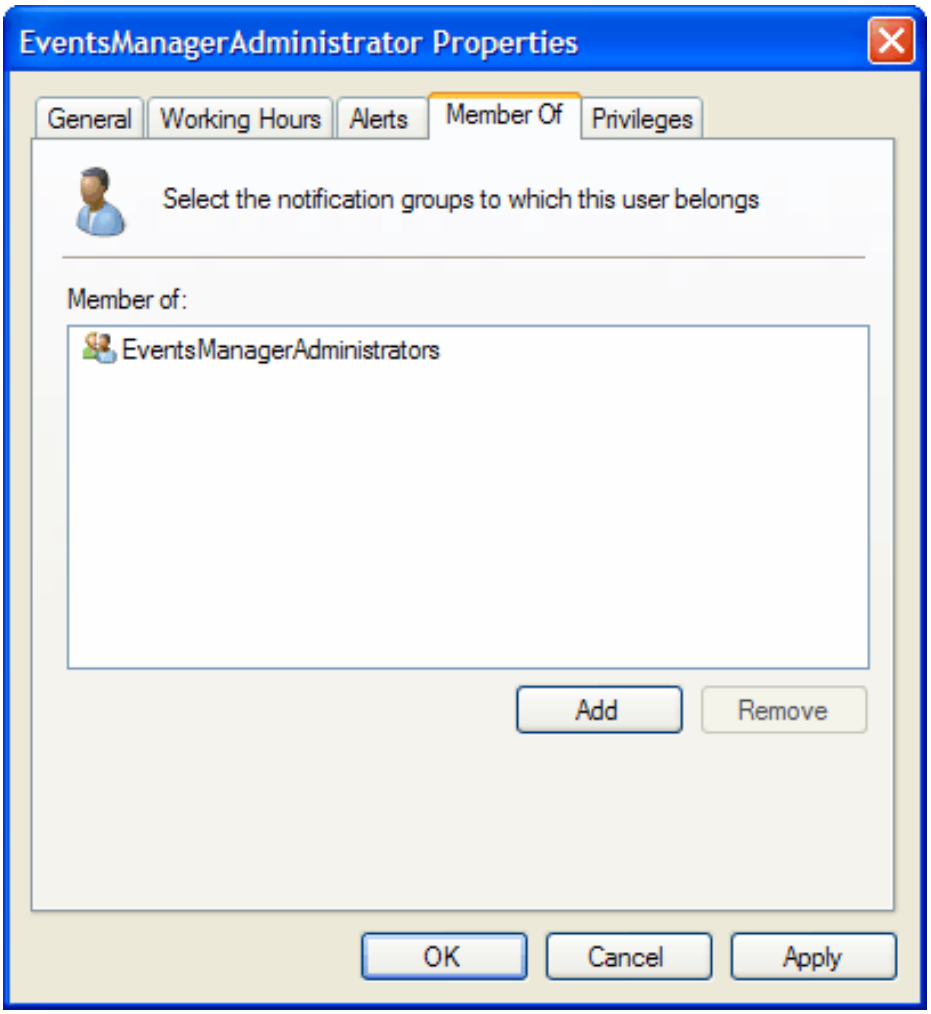
Screenshot 103 - Configuring the typical working hours of an alert recipient

4. Select the typical working hours of the administrator/user.



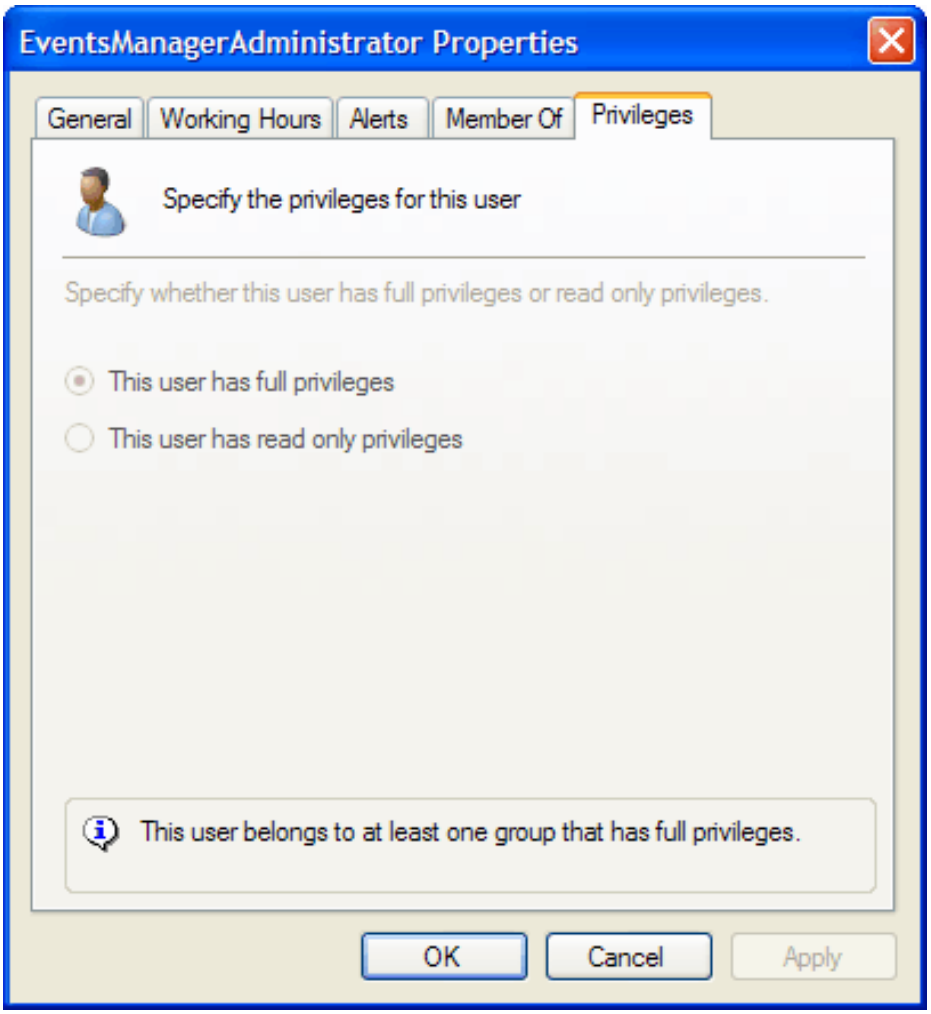
Screenshot 104 - Selecting alerts to be sent during and outside working hours

5. Click on the **Alerts** tab and select which alerts will be sent during and outside working hours.



Screenshot 105 - Notification groups to which a user belongs

6. Click on the **Member Of** tab and select the notification groups to which the user belongs. By default the administrator is a member of the 'EventsManagerAdministrators' notification group.



Screenshot 106 - Configuring GFI EventsManager administrator privileges

7. Click on **Privileges** tab and select **This user has full privileges** option.

8. Click on the **OK** button to finalize your settings.

10.3 Creating a new user

GFI EventsManager allows you to create a custom list of users which you can organize into groups to speed up administrative tasks.

To create a new user:

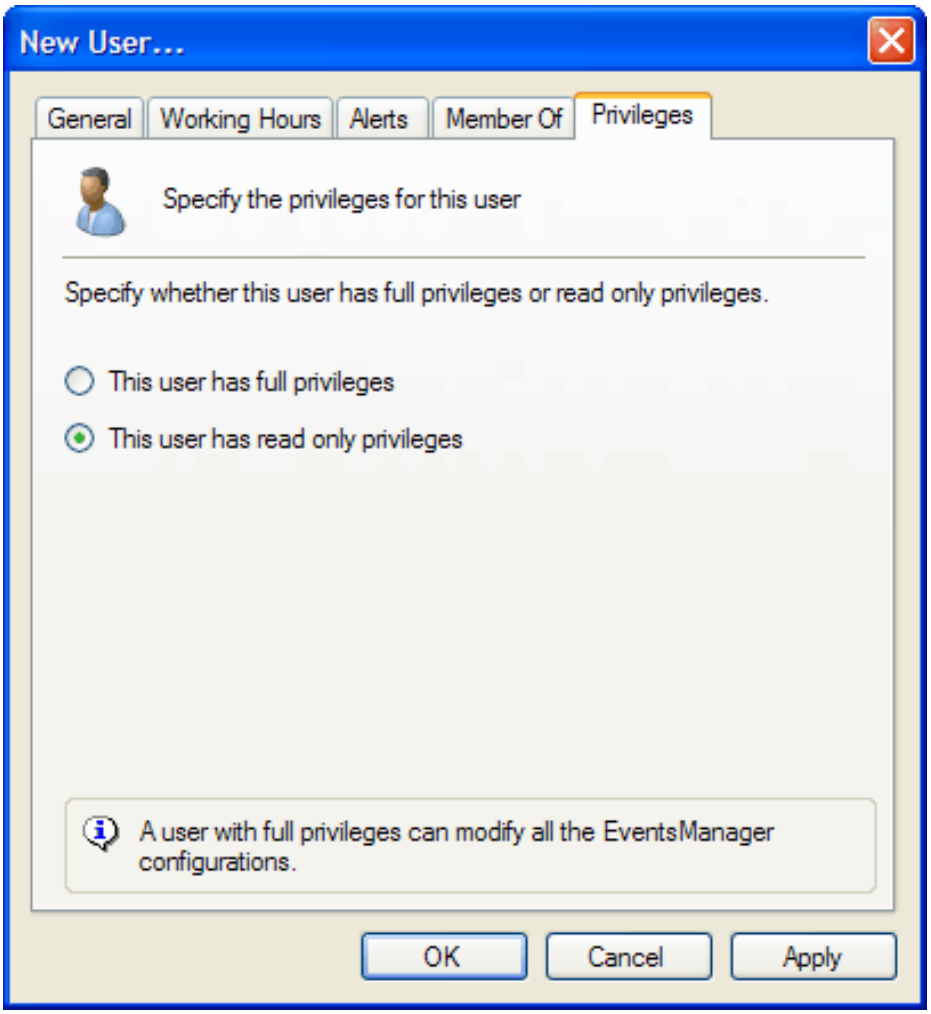
1. Click on the **Configuration** tab and select **Options**.

2. Expand the **Users and Groups** node.

3. Right-click on the **Users** sub-node and select **Create user…**

4. Specify the parameters requested in the **General**, **Working Hours**, **Alerts Member of** and **Privileges** tabs.

NOTE: For more information on how to fill in these tabs, refer to the 'Configuring the administrator account' section in this chapter.



Screenshot 107 - GFI EventsManager new user privileges

5. Click on the **Privileges** tab and select user privileges accordingly. E.g. To assign administrative privileges to a user select the **This user has full privileges** option.

NOTE: Users with administrative privileges can modify all GFI EventsManager configuration settings.

6. Click **OK** to finalize setup.

10.4 Changing user properties

To edit user properties:

1. From the left pane, click on the **Users** node.

2. Right-click on the user to edit and select **Properties**.

3. Make the required changes in the tabs available and click **OK** to finalize your settings.

NOTE: For more information on how to fill in these tabs, refer to the 'Configuring the administrator account' section in this chapter.

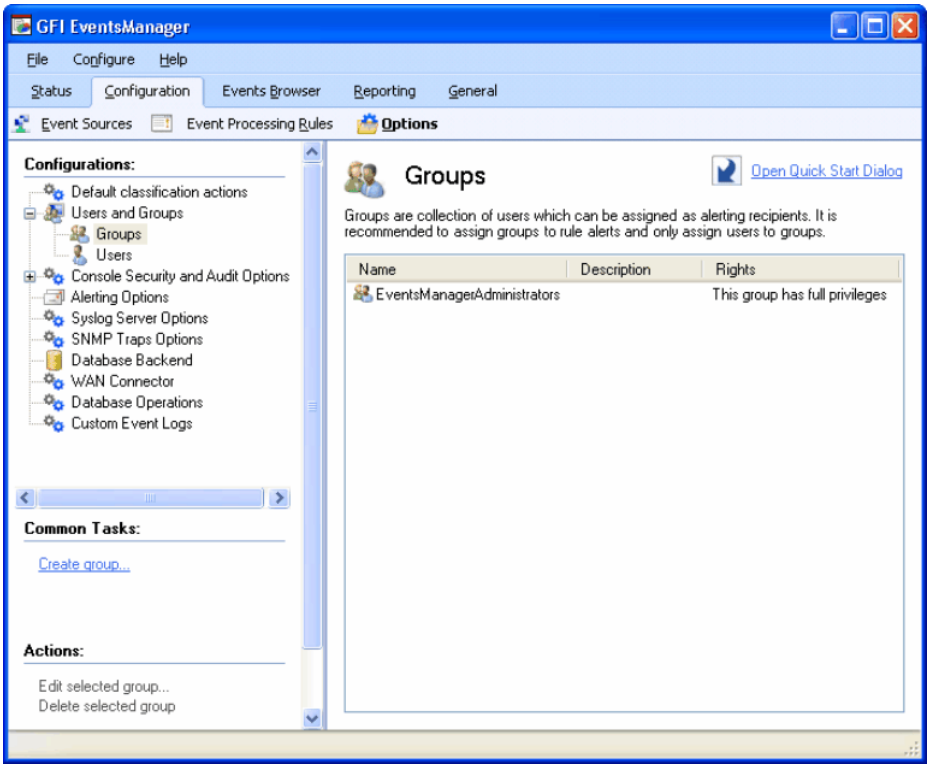
10.5 Deleting users

To delete a user:

1. From the left pane, click on the **Users** node.

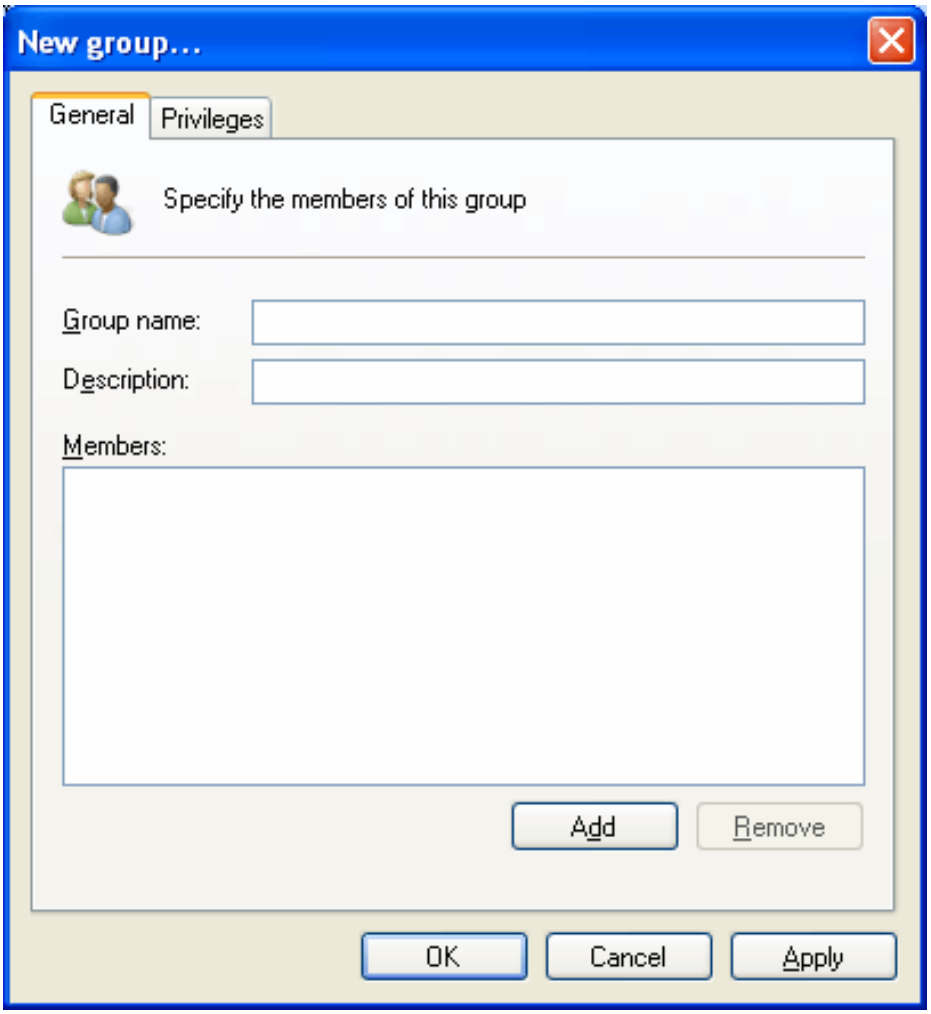
2. From the right viewer pane, right-click on the user to be deleted and select **Delete**.

10.6 Configuring groups



Screenshot 108 - Groups configuration screen

1. Click on the **Configuration** tab and select **Options**.
2. Expand the **Users and Groups** node.
3. Right-click on the **Groups** sub-node and select **Create group…**



Screenshot 109 - New groups setup

4. Specify the name of the new group.

5. Click **Add** to start adding users to the group.

6. Click **OK** to finalize your settings.

10.6.1 Changing user group properties

To edit the settings of a user group do as follows:

1. From the left pane, click on the **Groups** node.

2. From the right pane, right-click on the group to be configured and select **Properties**.

3. Perform the required changes in the tabs available and click **OK** to finalize your settings.

10.6.2 Deleting user groups

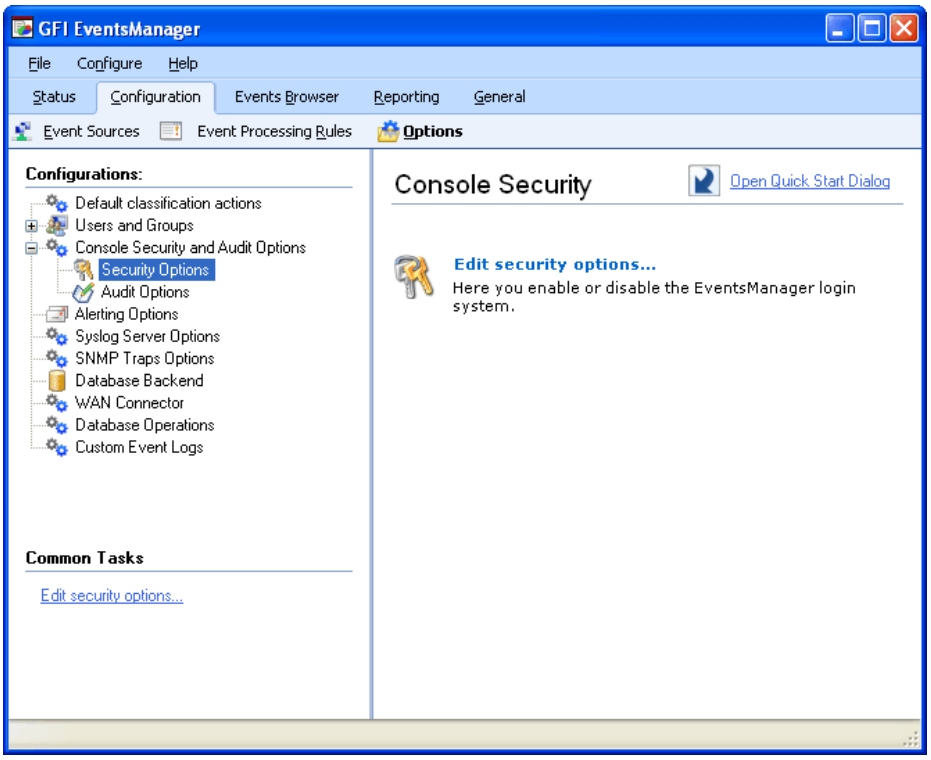
To delete a user group:

1. From the left pane, click on the **Groups** node.

2. From the right viewer pane, right-click on the group to be deleted and select **Delete**.

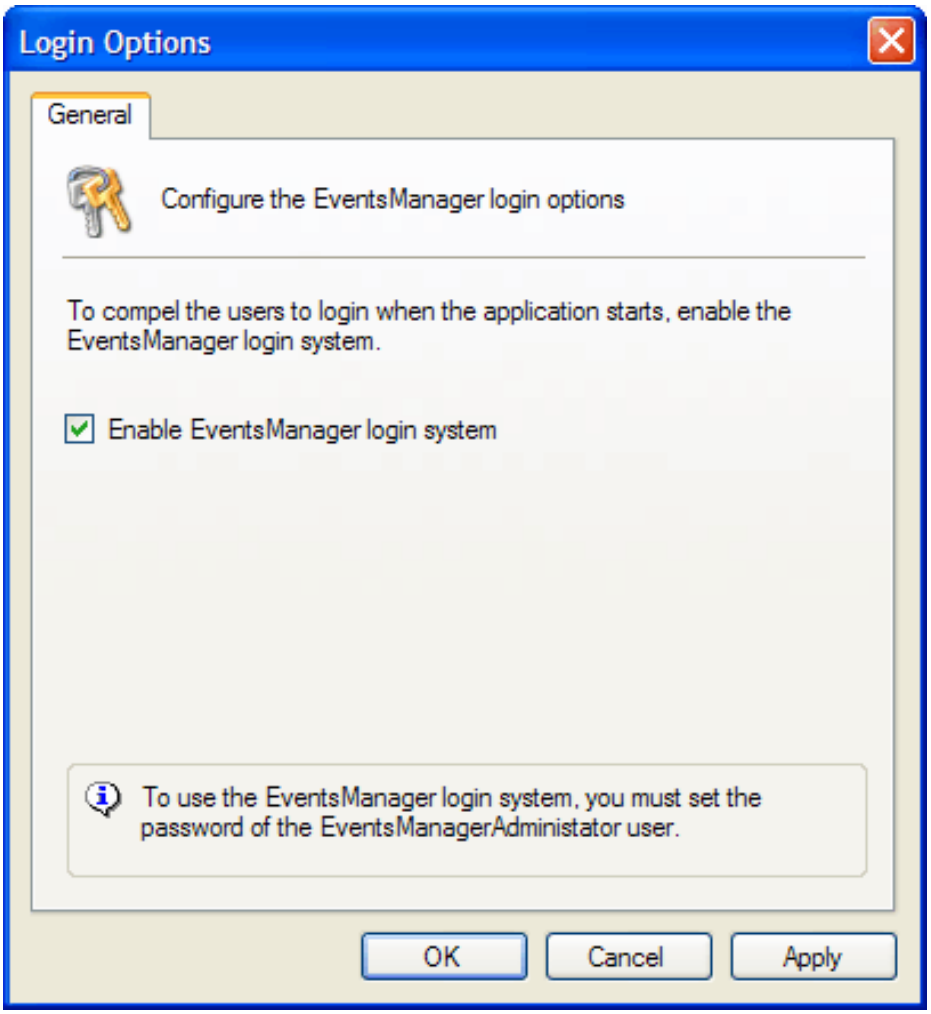
10.7 Enabling and disabling the GFI EventsManager login system

1. Click on the **Configuration** and select **Options**.



Screenshot 110 - Select the login options feature

2. Expand the **Console Security and Audit Options** node, click on the **Security Options** node and select **Edit security options…**.


Login Options
General
Configure the EventsManager login options
To compel the users to login when the application starts, enable the EventsManager login system.
Enable EventsManager login system
To use the EventsManager login system, you must set the password of the EventsManagerAdministator user.
OK
Cancel
Apply

Screenshot 111 - Login options dialog

3. Select/unselect the Enable EventsManager login system option accordingly.

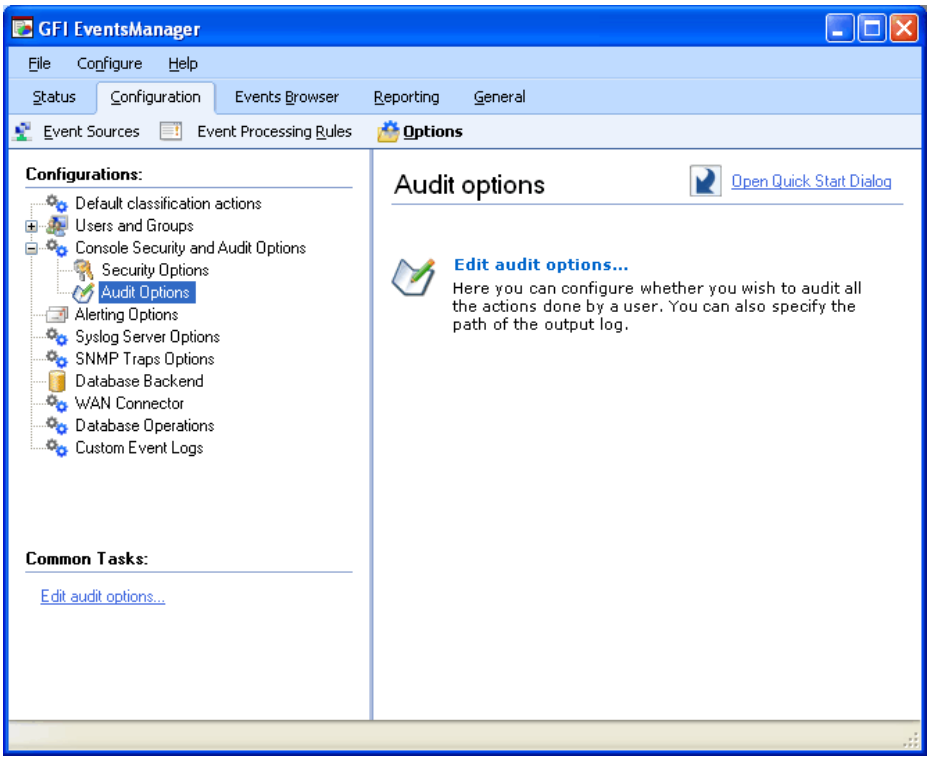
4. Click **OK** to finalize your settings.

NOTE 1: When the login system is enabled all users will be asked to specify their credentials every time they launch the GFI EventsManager management console.

NOTE 2: Users are granted access with administrative or user privileges according to the user privileges set up in the privileges tab within the user setup dialogs.

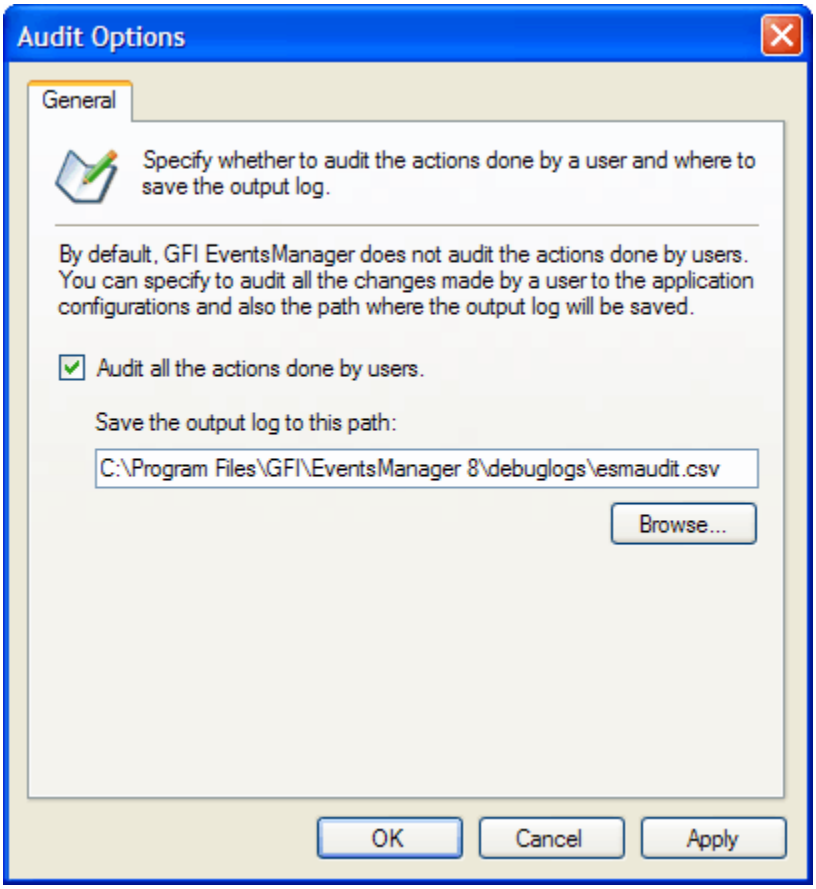
10.8 Enabling and disabling user action auditing

1. Click on the **Configuration** tab and select **Options**.



Screenshot 112 - Select the Audit options feature

2. Expand the **Console Security and Audit Options** node, click on the **Audit Options** node and select **Edit audit options…**.


Audit Options
General
Specify whether to audit the actions done by a user and where to save the output log.
By default, GFI EventsManager does not audit the actions done by users. You can specify to audit all the changes made by a user to the application configurations and also the path where the output log will be saved.
Audit all the actions done by users.
Save the output log to this path:
C:\Program Files\GFI\EventsManager 8\debuglogs\esmaudit.csv
Browse...
OK
Cancel
Apply

Screenshot 113 - Audit Options

3. Select **Audit all the actions done by users** option and specify the location where the output log file will be saved.

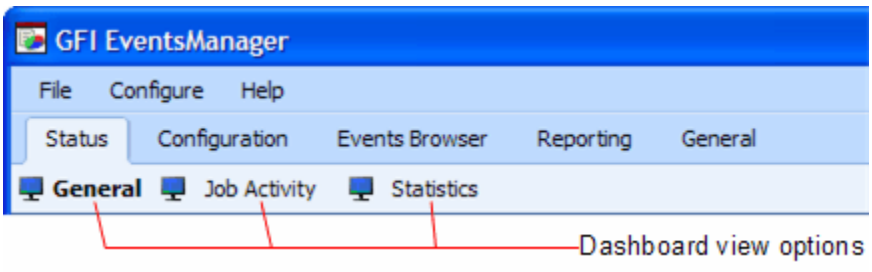
4. Click **OK** to finalize settings.

11 Status monitoring

11.1 Introduction

The status monitor is a dashboard that shows the status of GFI EventsManager as well as provides you with statistical information related to the events collected, processed and archived by this product. The status monitor consists of three different dashboard views: General view, Job Activity view and Statistics view.

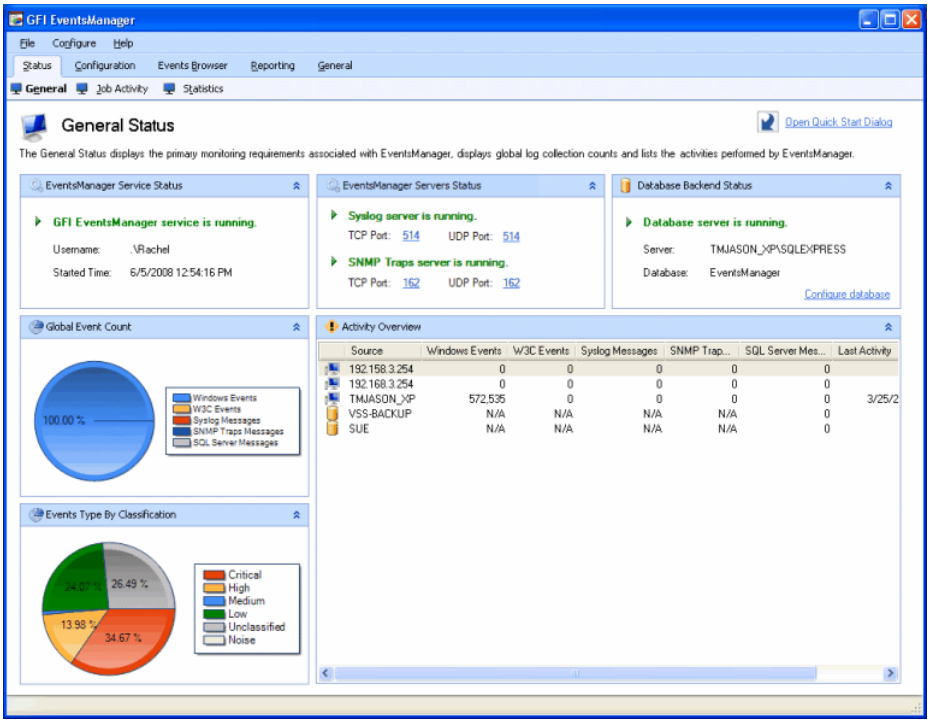
11.2 Accessing the status monitor



Screenshot 114 - Dashboard View Options

To access the status monitor click on the **Status** tab and select the required dashboard view. More detail about the dashboard view is provided in the coming sections.

11.3 General status view



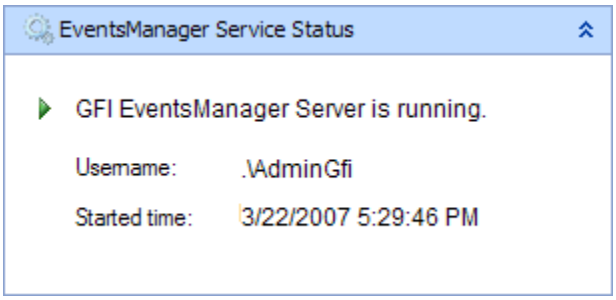
Screenshot 58 - GFI EventsManager status: General view

Use the **General** option to:

- View the status of the GFI EventsManager event processing engine.
- Access statistical information such as the number of events processed on a computer by computer basis.

The information provided in this view is divided into dedicated sections. More details on these sections are provided below.

EventsManager service status



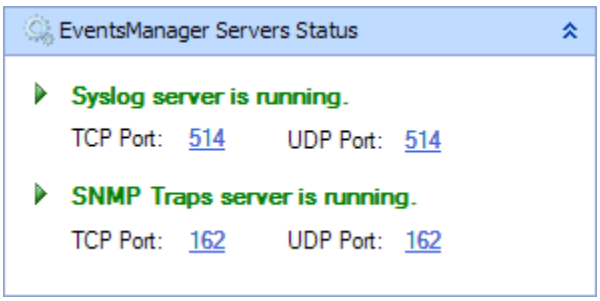
Screenshot 115 - GFI EventsManager General Status view: Service Status

This section shows:

- The operational status of GFI EventsManager service/event processing engine
- The user account under which the GFI EventsManager engine is running
- The time when the event processing service was started.

IMPORTANT: The GFI EventsManager service will not start if no database backend is currently configured.

EventsManager servers status

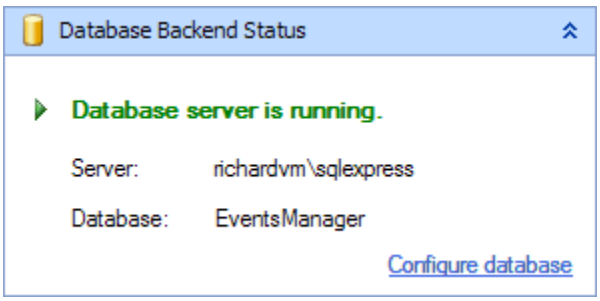


Screenshot 116 - GFI EventsManager General Status view: EventsManager Servers status

This section shows:

- The operational status of the Syslog server
- The Syslog server messaging/communication port.
- The operational status of the SNMP Traps server
- The SNMP Traps server messaging/communication port.

Database backend status

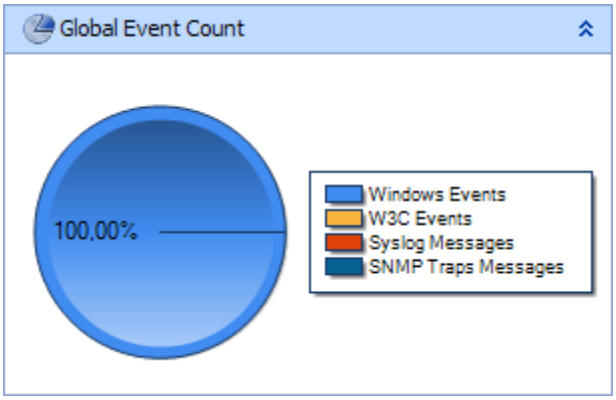


Screenshot 117 - GFI EventsManager General Status view: Database Backend Status

This section shows:

- The operational status of the database server currently in use by GFI EventsManager
- The name of the database server currently in use by GFI EventsManager
- The name of the database in which GFI EventsManager is archiving collected events.

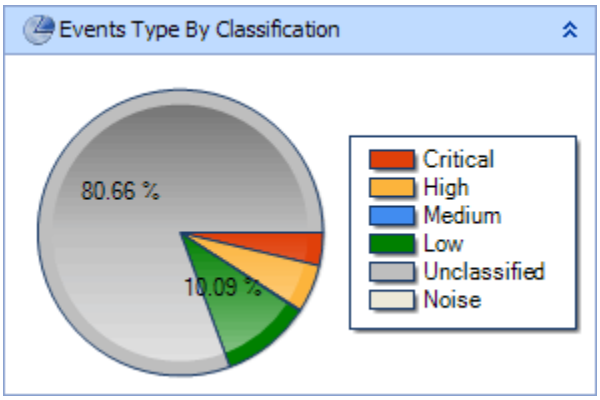
Global event count



Screenshot 118 - GFI EventsManager General Status view: Global Event Count

This section graphically represents the percentage number of Windows, W3C, Syslog and SNMP Trap messages processed by GFI EventsManager.

Events type by classification

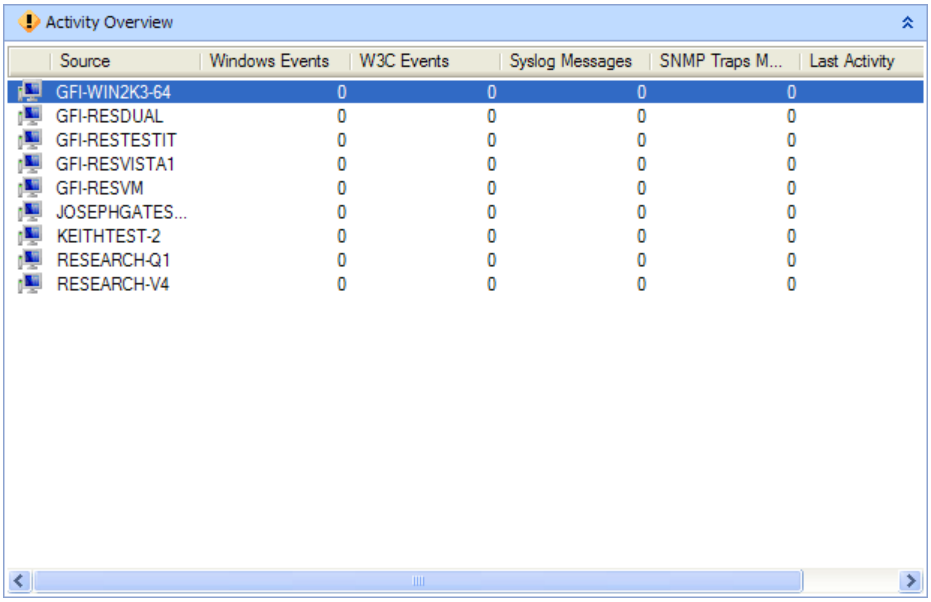


Screenshot 119 - GFI EventsManager General Status view: Events Type by Classification

This section graphically represents the percentage number of events that were:

- Classified as **Critical**, **High**, **Medium** or **Low**
- Unclassified.

Activity overview

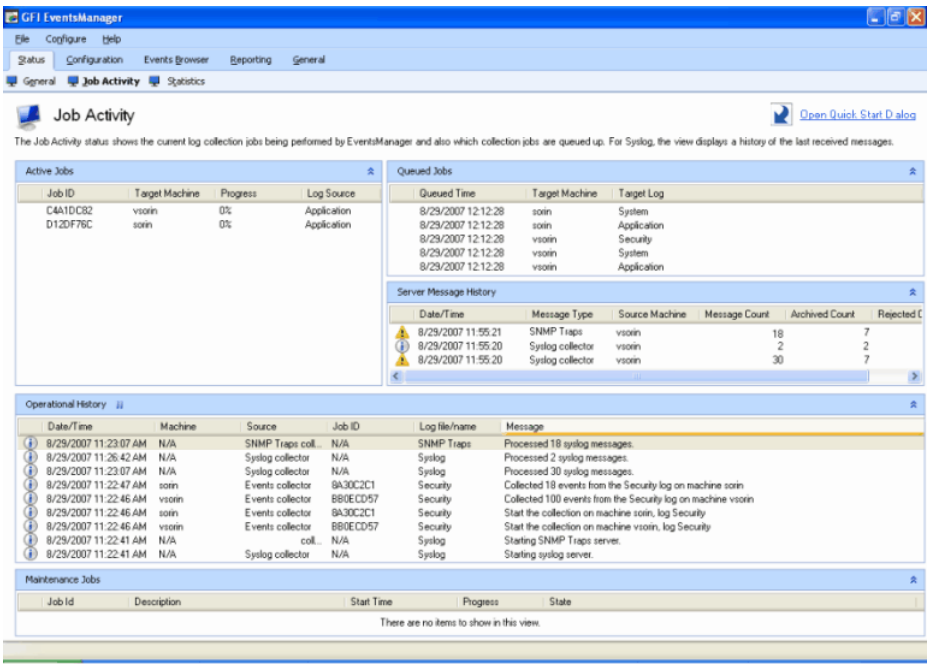


Screenshot 120 - GFI EventsManager General Status view: Activity Overview

This section shows:

- The total number of Windows, W3C, Syslog and SNMP Traps events processed on a machine by machine basis
- The date/time of the last event collection performed from every machine.

11.4 Job activity view

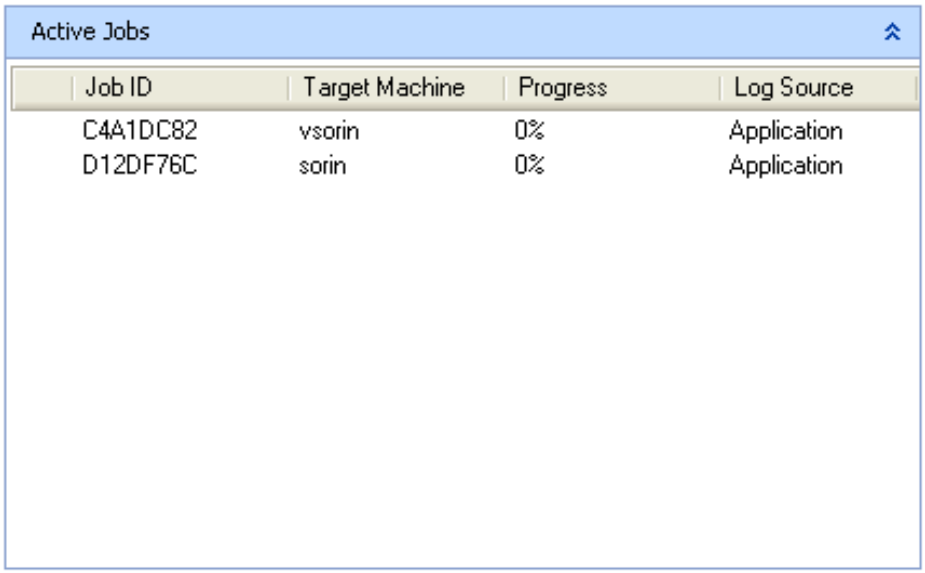

GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
General Job Activity Statistics
Job Activity
Open Quick Start Dialog
The Job Activity status shows the current log collection jobs being performed by EventsManager and also which collection jobs are queued up. For Syslog, the view displays a history of the last received messages.
Active Jobs
Job ID Target Machine Progress Log Source
C4A1DC82 vsorin 0% Application
D12DF76C sorin 0% Application
Queued Jobs
Queued Time Target Machine Target Log
8/29/2007 12:12:28 sorin System
8/29/2007 12:12:28 sorin Application
8/29/2007 12:12:28 vsorin Security
8/29/2007 12:12:28 vsorin System
8/29/2007 12:12:28 vsorin Application
Server Message History
Date/Time Message Type Source Machine Message Count Archived Count
8/29/2007 11:55:21 SNMP Traps vsorin 18 7
8/29/2007 11:55:20 Syslog collector vsorin 2 2
8/29/2007 11:55:20 Syslog collector vsorin 30 7
Operational History
Date/Time Machine Source Job ID Log file/name Message
8/29/2007 11:23:07 AM N/A SNMP Traps coll... N/A SNMP Traps Processed 18 syslog messages.
8/29/2007 11:26:42 AM N/A Syslog collector N/A Syslog Processed 2 syslog messages.
8/29/2007 11:23:07 AM N/A Syslog collector N/A Syslog Processed 30 syslog messages.
8/29/2007 11:22:47 AM sorin Events collector 8A30C2C1 Security Collected 18 events from the Security log on machine sorin
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Collected 100 events from the Security log on machine vsorin
8/29/2007 11:22:46 AM sorin Events collector 8A30C2C1 Security Start the collection on machine sorin, log Security
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Start the collection on machine vsorin, log Security
8/29/2007 11:22:41 AM N/A coll... N/A Syslog Starting SNMP Traps server.
8/29/2007 11:22:41 AM N/A Syslog collector N/A Syslog Starting syslog server.
Maintenance Jobs
Job Id Description Start Time Progress State
There are no items to show in this view.

Screenshot 121 - GFI EventsManager Job Activity view

Use the **Job Activity** option to view your current event collection and processing activity. This includes active event collection jobs as well as Syslog messaging history on a machine by machine.

The information provided in this view is divided into dedicated sections. More details on these sections are provided below.

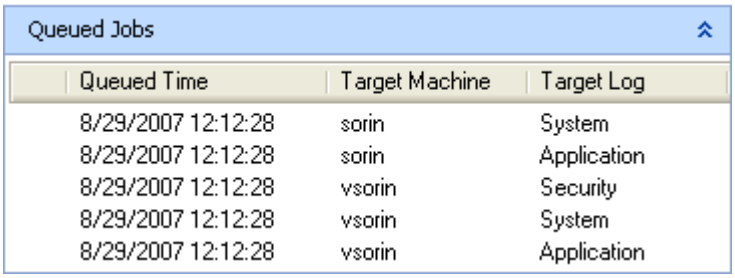
Active jobs



Screenshot 122 - GFI EventsManager Job Activity view: Active Jobs

This section shows a list of all event collection jobs currently taking place on every event source/machine. The information provided includes the job progress as well as the Log Source from which events are being collected.

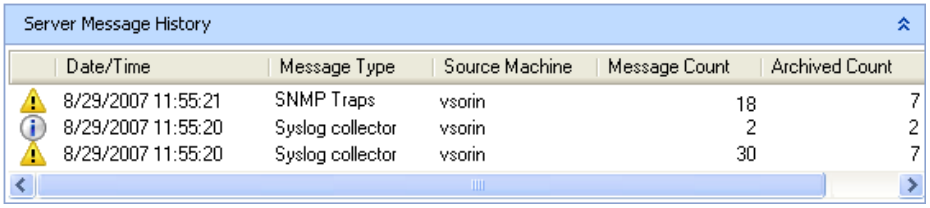
Queued jobs



Screenshot 123 - GFI EventsManager Job Activity view: Queued Jobs

This section shows a list of all pending event collection jobs on a machine by machine basis. The information provided includes the Log Source from which events will be collected as well as the time that these jobs were queued.

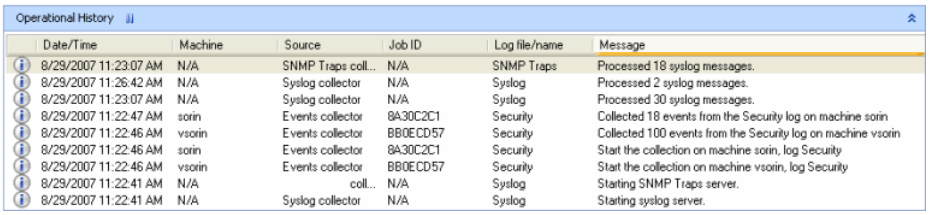
Server message history



Screenshot 124 - GFI EventsManager Job Activity view: Server Message History

This section shows a list of all server messages (SNMP Traps and Syslog) that were received by GFI EventsManager. The information provided includes the total number of messages sent by every source machine and the date/time when the last message was received.

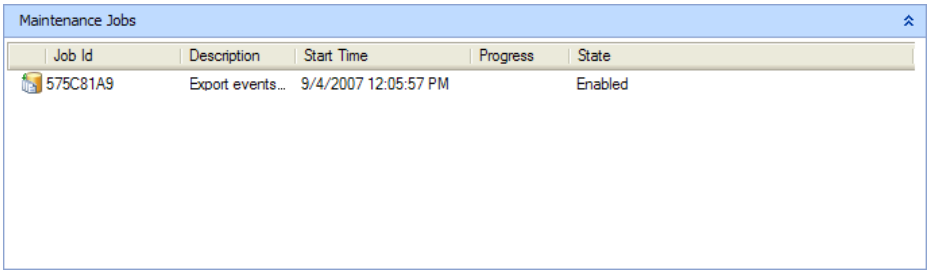
Operational history


Operational History
Date/Time Machine Source Job ID Log file/name Message
8/29/2007 11:23:07 AM N/A SNMP Traps coll... N/A SNMP Traps Processed 18 syslog messages.
8/29/2007 11:26:42 AM N/A Syslog collector N/A Syslog Processed 2 syslog messages.
8/29/2007 11:23:07 AM N/A Syslog collector N/A Syslog Processed 30 syslog messages.
8/29/2007 11:22:47 AM sorin Events collector 8A30C2C1 Security Collected 18 events from the Security log on machine sorin
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Collected 100 events from the Security log on machine vsorin
8/29/2007 11:22:46 AM sorin Events collector 8A30C2C1 Security Start the collection on machine sorin, log Security
8/29/2007 11:22:46 AM vsorin Events collector BB0ECD57 Security Start the collection on machine vsorin, log Security
8/29/2007 11:22:41 AM N/A coll... N/A Syslog Starting SNMP Traps server.
8/29/2007 11:22:41 AM N/A Syslog collector N/A Syslog Starting syslog server.

Screenshot 125 - GFI EventsManager Job Activity view: Operational History

This section shows an audit trail of the event collection operations carried out by GFI EventsManager. The information provided includes errors and information messages generated during the event collection process as well as the name of the log file that was being processed on the source machine.

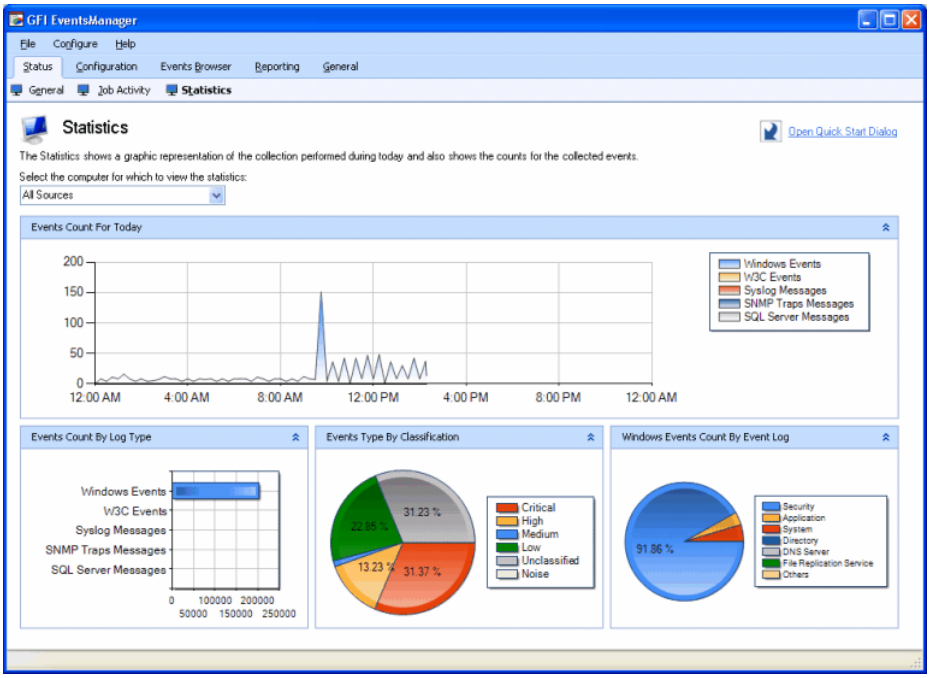
Maintenance jobs



Screenshot 126 - GFI EventsManager Job Activity view: Job activity status

This section shows the progress of maintenance jobs that have been created through **Database Operations**. The information provided includes the job description as well as the time when the job began execution.

11.5 Statistics view

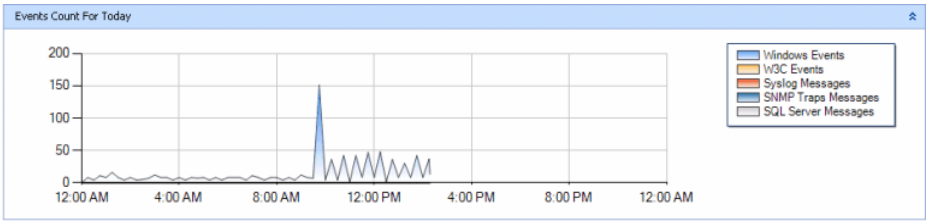


Screenshot 127 - GFI EventsManager Statistics view

Use the **Statistics** option to view the daily event activity trends and statistics of a particular computer or of your entire network.

The information provided in this view is divided into dedicated sections. More details on these sections are provided below.

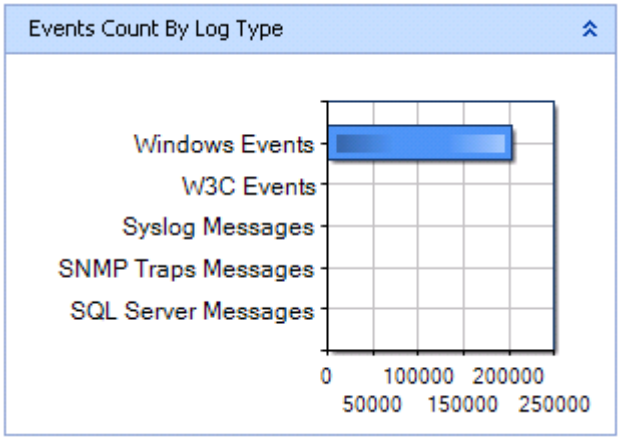
Events count for today



Screenshot 128 - GFI EventsManager Statistics view: Events Count For Today

This section graphically represents the daily event collection trend on a machine by machine basis as well as on a network by network basis. A color scheme is used to differentiate between Windows, W3C, Syslog and SNMP Traps events.

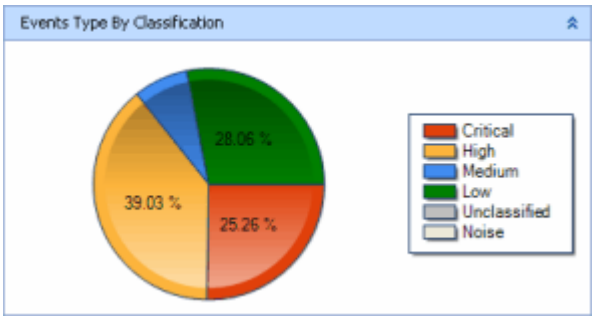
Events count by log type



Screenshot 129 - GFI EventsManager Statistics view: Events count by log type

This section graphically represents the number of Windows, W3C, Syslog and SNMP Traps events collected by GFI Events Manager from a particular machine or network.

Events count by classification

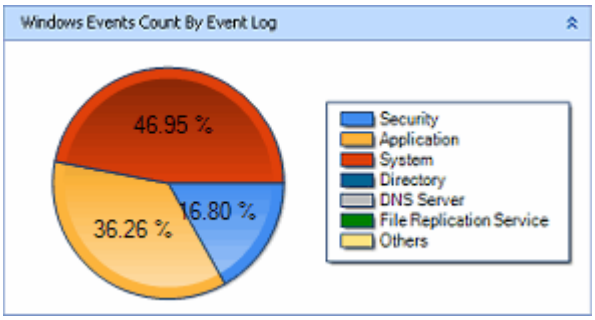


Screenshot 130 - GFI EventsManager Statistics view: Events Count by Classification

This section graphically represents (on a machine or network wide level) the percentage number of events that were:

- Classified as **Critical**, **High**, **Medium** or **Low**
- Unclassified.

Windows events count by event log



Screenshot 131 - GFI EventsManager Statistics view: Windows Events Count by Event Log

This section graphically represents the percentage number of Windows events collected from the Security, System, Application, DNS Server, Directory, File Replications Service and other logs.

12 Database Operations

12.1 Introduction

The Database Operations module in GFI EventsManager provides advanced functionality allowing administrators to:

- Centralize events collected by other remote GFI EventsManager instances into one database backend.
- Optimize GFI EventsManager performance by actively controlling database backend growth hence keeping it in good shape.
- Import and export data to and from GFI EventsManager version 8.x installations without data inconsistencies.

12.2 Why is there a need for database maintenance?

Periodical database maintenance is essential in preventing excessive data growth in the database backend. A database which is large in size drastically affects the performance of GFI EventsManager; events browsing will be slower and queries will take longer to execute. There will also be a negative impact on GFI EventsManager ReportPack performance, with reports taking longer to be generated.

Through GFI EventsManager a number of database operations, referred to as maintenance jobs, can be carried out on the database backend. These include:

- Move to database - Use this operation to move events from the main database to the backup database or to another existing database.
- Export to file - Use this operation to export events from the main database to a compressed binary file which can also be encrypted and backed to CD/DVD or tape for safekeeping.
- Import from file - Use this operation to import events from GFI EventsManager export files into the main database backend.
- Delete data - Use this operation to remove events from the main or backup database back-ends.

For each of these operations, you can also apply filters that determine which events will be affected by the database operation.

Consolidation of events for a WAN

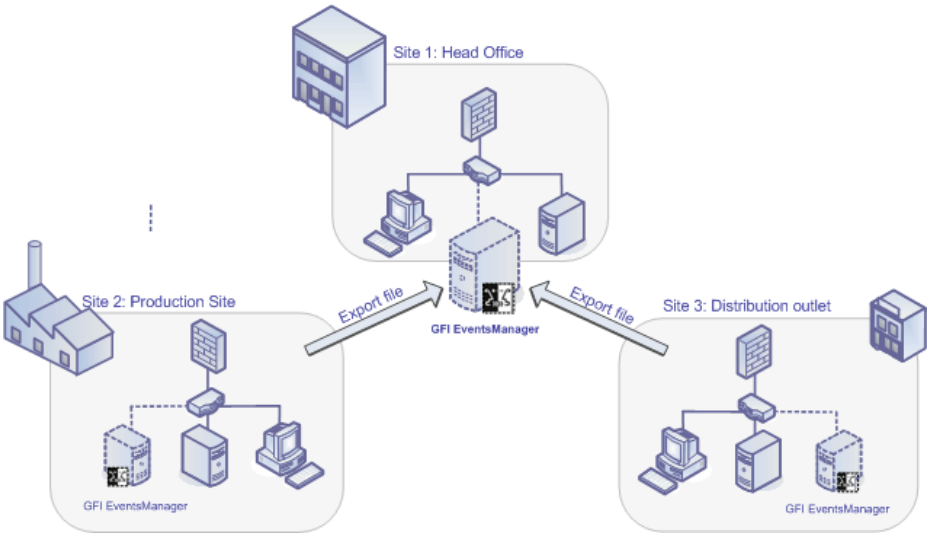


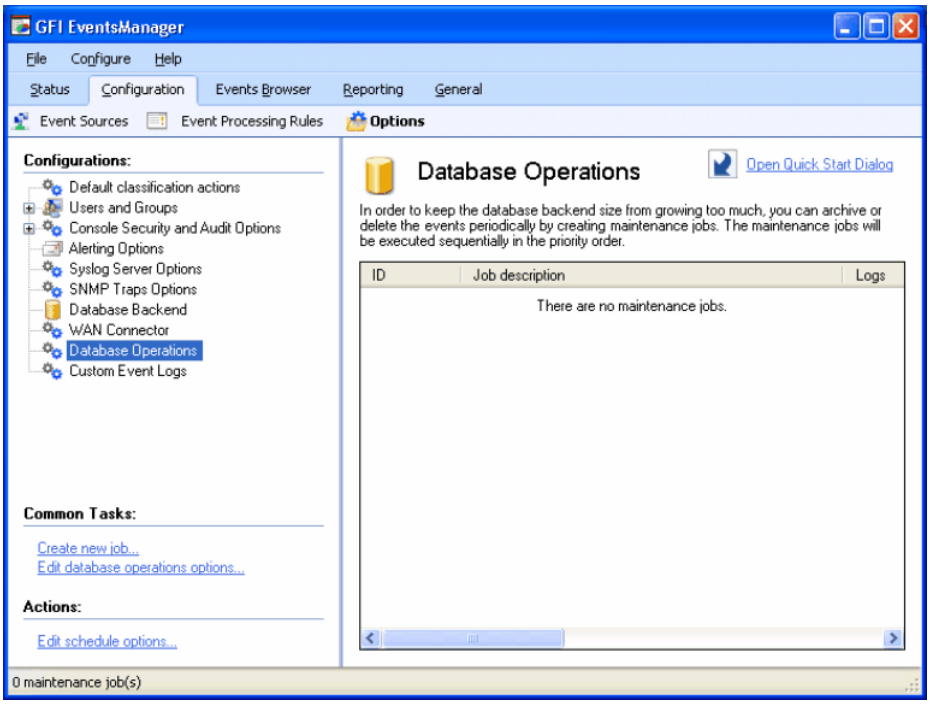
Figure 1: Consolidation of events for a WAN

In the case of organizations with remote geographical sites, Database Operations can be used to consolidate all or part of the events data collected in remote sites on to one central database. This is achieved using the 'Export to file' feature through which GFI EventsManager compresses and encrypts the file as well as export the file to be processed to a central location. The 'Import to file' job is executed at the central location, importing the events from the remote site into the central database.

Events for the remote site can then be viewed through the Events Browser. Reports with information relevant to the remote site can also be generated using data from the central database.

12.3 Configuring Database Operations

With GFI EventsManager you can schedule maintenance jobs to be executed on a specific day, at a specific time and at specific intervals.



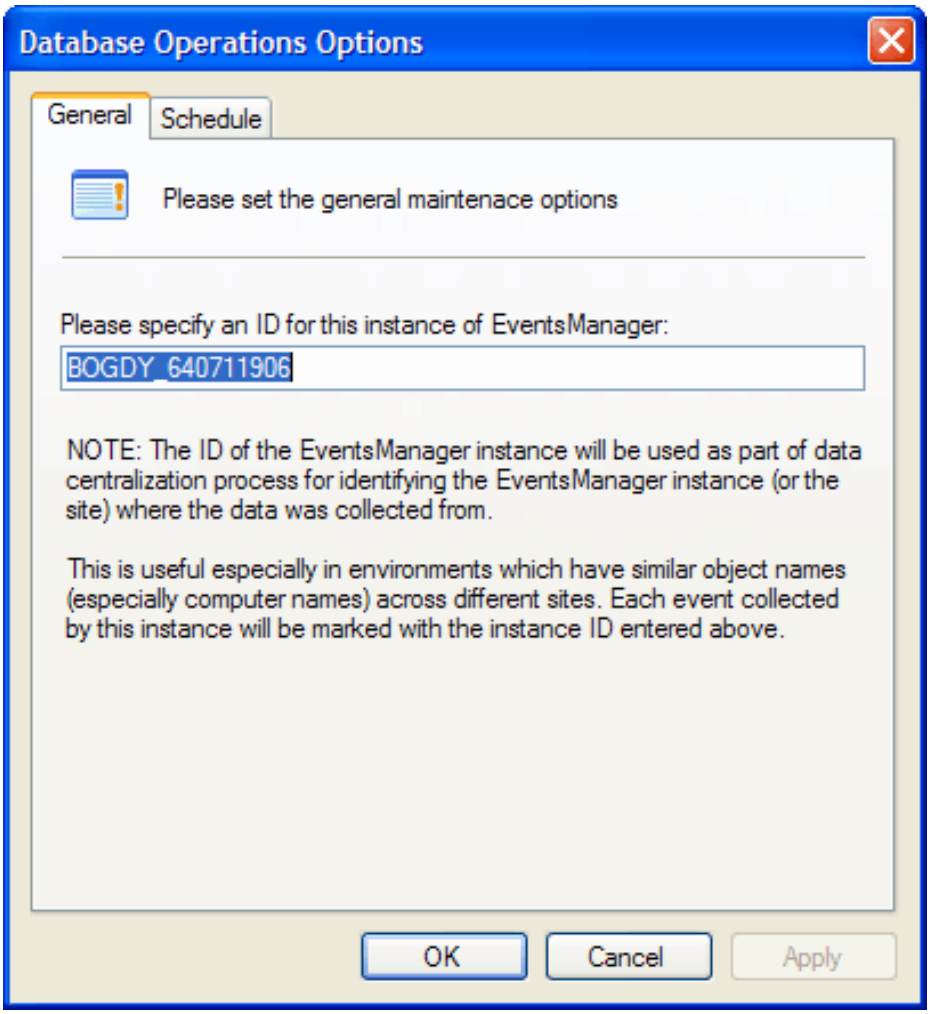
Screenshot 132 - Configuring Database Operations

NOTE: Database maintenance operations may require high utilization of resources which can degrade server and GFI EventsManager performance. Thus, it is recommended that you schedule maintenance jobs to be executed after office hours. This allows you to maximize the availability of your system resources during working hours and avoid any possible disruptions to workflow.

To configure Database Operations:

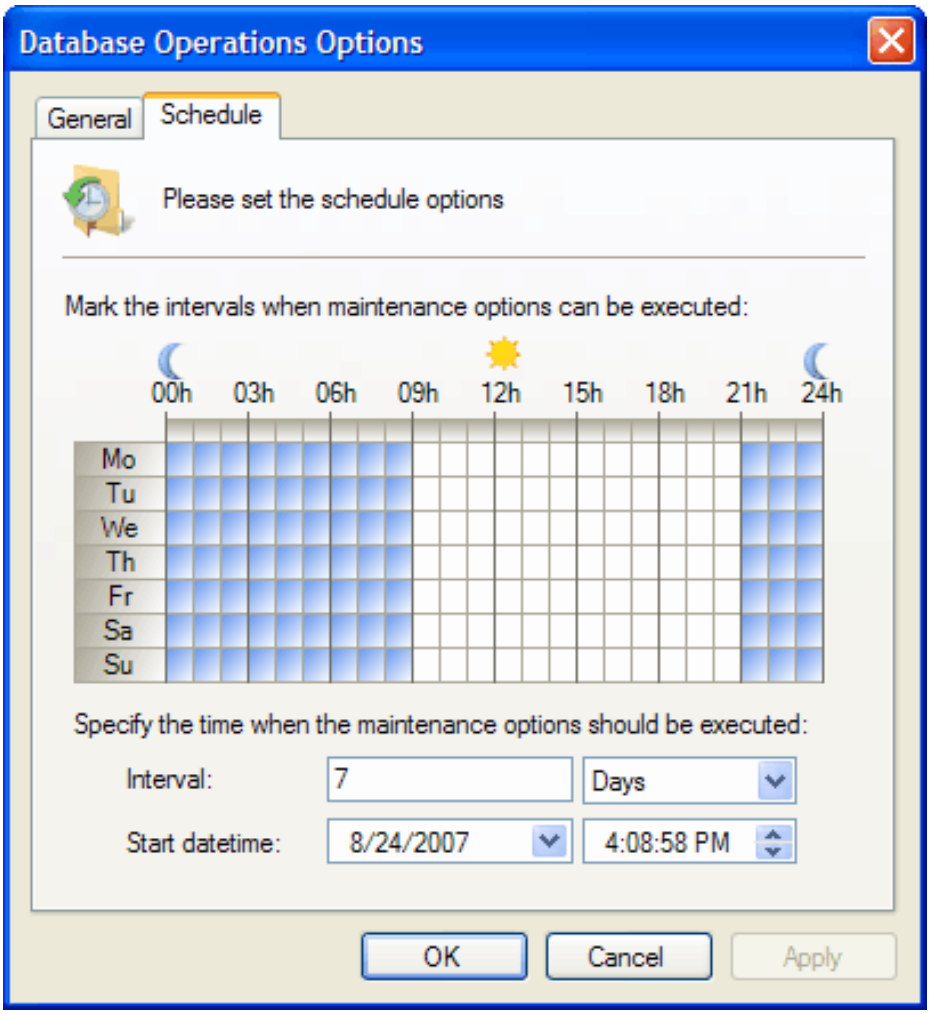
1. Click on the **Configuration** tab and select **Options**.

2. From the left pane, right-click on the **Database Operations** node and select **Properties**.


Database Operations Options
General
Schedule
Please set the general maintenace options
Please specify an ID for this instance of EventsManager:
BOGDY_640711906
NOTE: The ID of the EventsManager instance will be used as part of data centralization process for identifying the EventsManager instance (or the site) where the data was collected from.
This is useful especially in environments which have similar object names (especially computer names) across different sites. Each event collected by this instance will be marked with the instance ID entered above.
OK
Cancel
Apply

Screenshot 133 - Database Operations Options dialog: GFI EventsManager unique identifier

3. Specify the unique identifier by which this instance of GFI EventsManager will be identified on the network. This identifier is used as part of the export file-name during 'Export to file' operations.



Screenshot 134 - Database Operations Options dialog: Scheduling options

4. Click on the **Schedule** tab to specify:

- Hours of the day during which maintenance jobs can be executed
- The interval in hours/days with which maintenance jobs will be executed
- The scheduled date/time when maintenance jobs will start being executed.

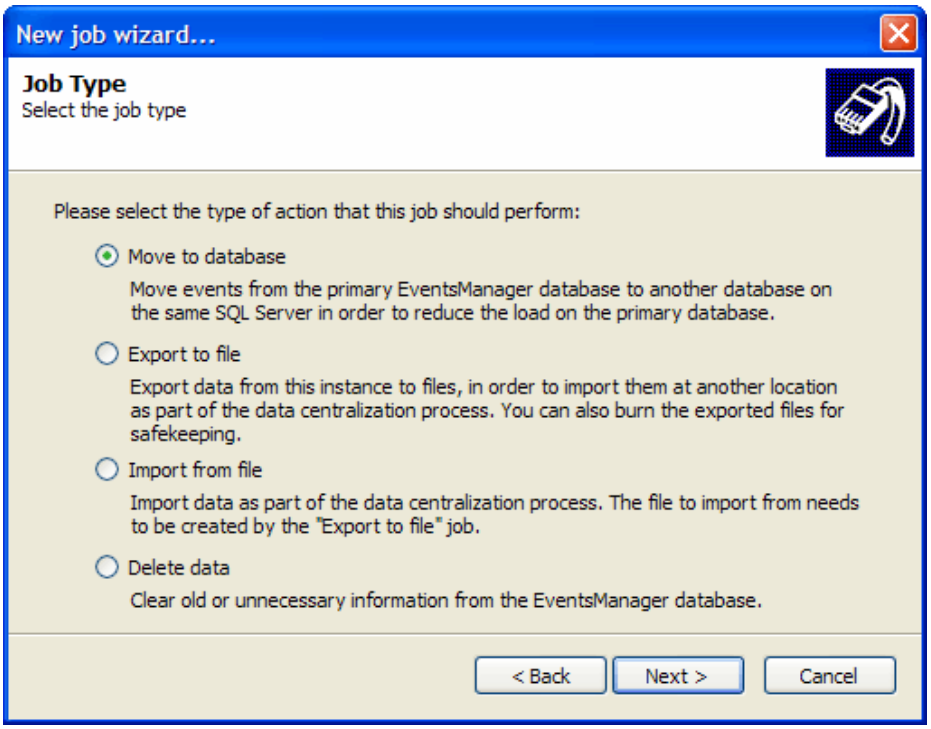
12.4 Creating maintenance jobs

To create a new maintenance job:

1. Click on the **Configuration** tab and select **Options**.

2. From the left pane, right-click on the **Database Operations** node and select **Create new job…** This will bring up the 'New job wizard'.

3. As soon as the welcome dialog is displayed, click on the **Next** button to bring up the 'Job Type' dialog.

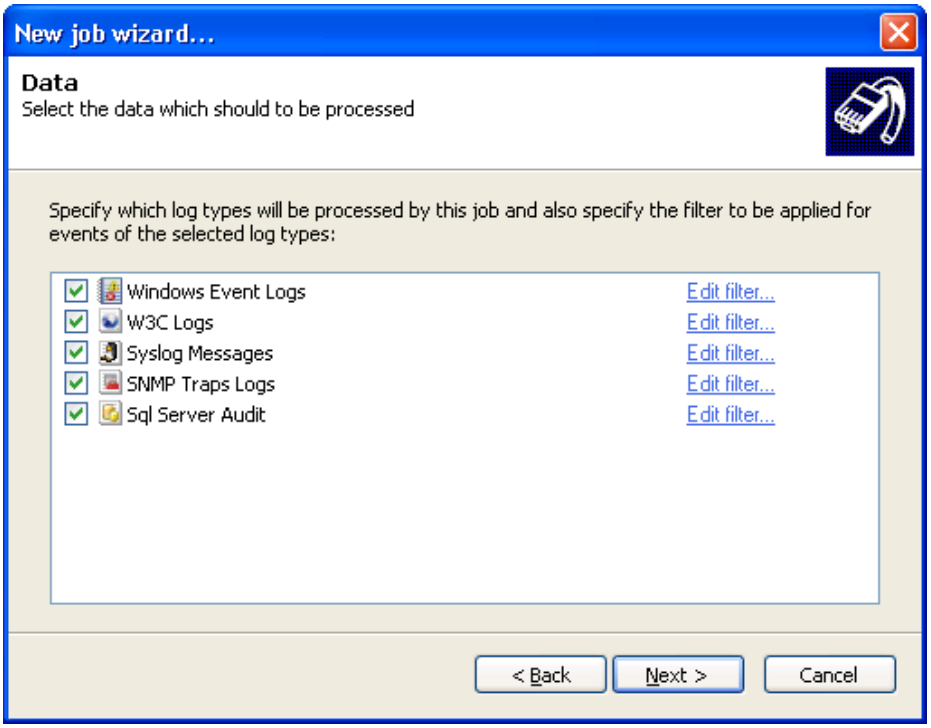

New job wizard...
Job Type
Select the job type
Please select the type of action that this job should perform:
Move to database
Move events from the primary EventsManager database to another database on the same SQL Server in order to reduce the load on the primary database.
Export to file
Export data from this instance to files, in order to import them at another location as part of the data centralization process. You can also burn the exported files for safekeeping.
Import from file
Import data as part of the data centralization process. The file to import from needs to be created by the "Export to file" job.
Delete data
Clear old or unnecessary information from the EventsManager database.
< Back
Next >
Cancel

Screenshot 135 - New job wizard: Job Type dialog

4. Select the type of maintenance job you want to create and click **Next** to proceed to the configuration dialog.

5. Specify the required parameters and click **Next** to proceed to the data filter configuration dialog.

NOTE: For information on how to configure the parameters of a particular maintenance job, refer to the relevant section in this chapter.


New job wizard...
Data
Select the data which should to be processed
Specify which log types will be processed by this job and also specify the filter to be applied for events of the selected log types:
Windows Event Logs
Edit filter...
W3C Logs
Edit filter...
Syslog Messages
Edit filter...
SNMP Traps Logs
Edit filter...
Sql Server Audit
Edit filter...
< Back
Next >
Cancel

Screenshot 136 - Data filter dialog: Specifying data filter conditions

6. Specify which data will be filtered from your database backend. If no filter is specified, the selected maintenance job will affect all data within your database backend. Click **Next** to continue.

NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this chapter.

New job wizard...
Completing the "New Job" Wizard
Select when the job should be executed:
Scheduled job
The job will be saved and executed according to the Enterprise Maintenance schedule options.
Run the job now
The job will be executed only once.
GFI
< Back
Finish
Cancel

Screenshot 137 - Specify when the job will be executed

7. Specify whether the selected maintenance job should be scheduled or executed immediately.

NOTE 1: Scheduled jobs are executed according to interval settings configured in the 'Database Operations'.

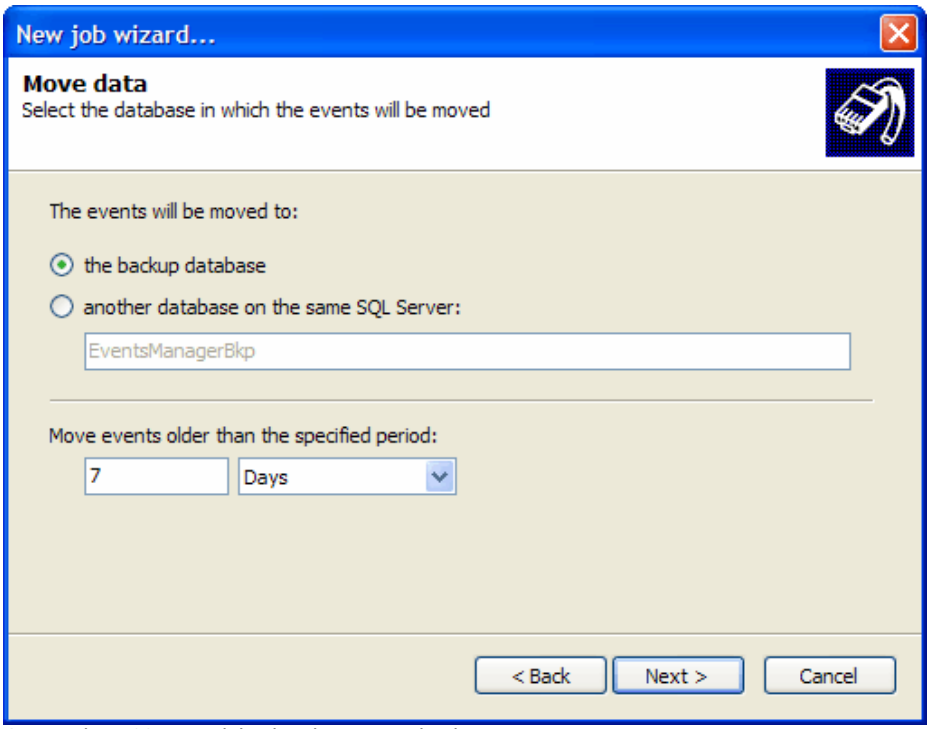
NOTE 2: Selected maintenance jobs will be executed only once.

8. Click **Finish** to finalize your configuration settings.

12.5 Move to database

To create a maintenance job which moves events between the main database and any other target database:

1. Launch the 'New job wizard' dialog; select the **Move to database** option.



Screenshot 138 - New job wizard: Move to database

2. Specify the database to which events will be moved. This should be either the backup database or another accessible database on the SQL Server hosting the main database.

3. Specify the frequency in hours/days at which events will be moved from the main database.

4. Click **Next** to bring up the data filter conditions dialog.

5. Configure the data filter conditions that will be applied for the 'Move to database' job. If you do not set any data filter conditions, than all events older than the specified period will be moved. Click **Next** to continue.

NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this chapter.

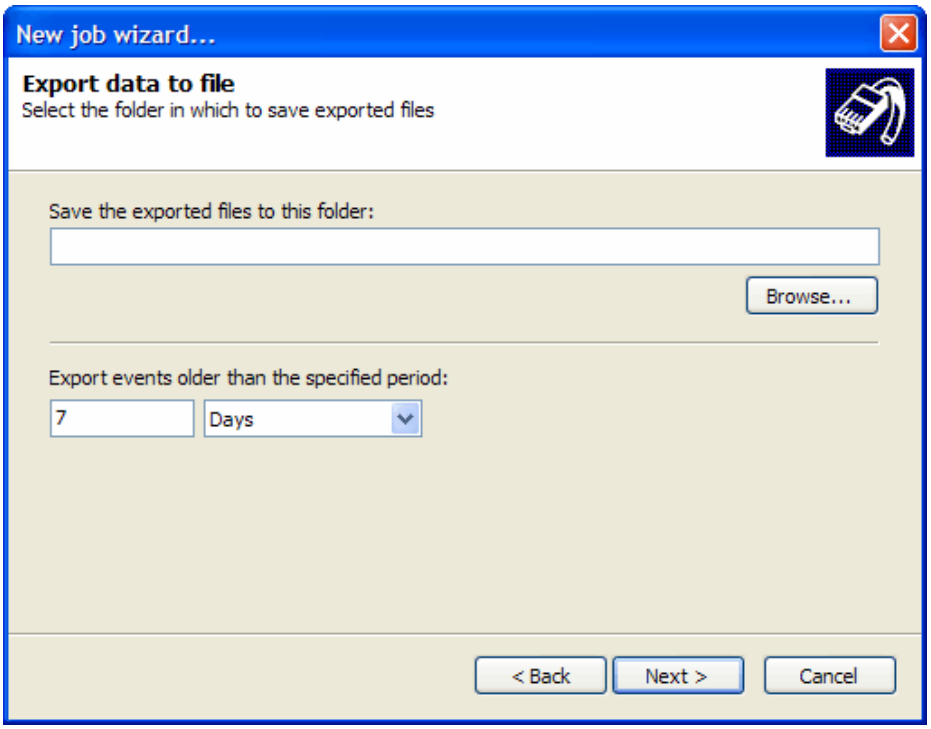
6. Specify whether the maintenance job should be scheduled or executed immediately.

7. Click on **Finish** to finalize configuration of the new 'Move to database' job.

12.6 Export to file

To export events from the main database to a binary file:

1. Launch the 'New job wizard' and select the **Export to file** option.



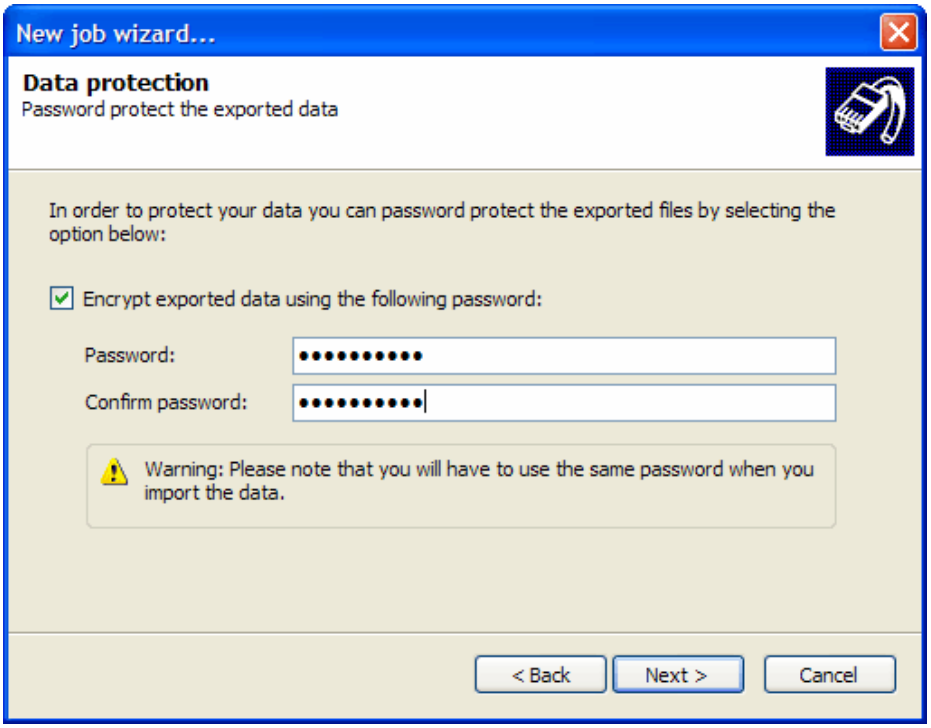
Screenshot 139 - New job wizard: Export to file

2. Specify the target folder where the exported file will be stored. Use the UNC notation to specify remote paths.

NOTE: Ensure that GFI EventsManager has administrative privileges over the specified target folder.

3. Specify the frequency in hours/days at which events will be exported from the main database.

4. Click **Next** to bring up the data protection dialog.


New job wizard...
Data protection
Password protect the exported data
In order to protect your data you can password protect the exported files by selecting the option below:
Encrypt exported data using the following password:
Password:
Confirm password:
Warning: Please note that you will have to use the same password when you import the data.
< Back
Next >
Cancel

Screenshot 140 - New job wizard: Export to file using encryption

5. Define whether the exported events data will be encrypted, specify the password to be used for decryption and click **Next** to proceed to the data filter dialog.

NOTE 1: It is recommended that files to be exported are always encrypted using strong passwords.

6. Configure the data filter conditions that will be applied for 'Export to file' jobs. If you do not set any data filter conditions, than all events older than the specified period will be exported. Click **Next** to continue.

NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this chapter.

7. Define whether the maintenance job should be scheduled or executed immediately.

8. Click on **Finish** to finalize your settings.

Export filename

The convention used by GFI EventsManager to name the export file is shown and described below:

- **[ESM ID]_[Job ID]_[Date From]_[Date To].EXP**
- **ESM ID** - refers to the unique identifier given to each GFI EventsManager instance running in the organization.
- **Job ID** - refers to the unique identifier given to each maintenance job created.
- **Date From** - refers to the date of the earliest event exported.
- **Date To** - refers to the date of the latest event exported.
- **.EXP** - this is the file extension given to all export files.

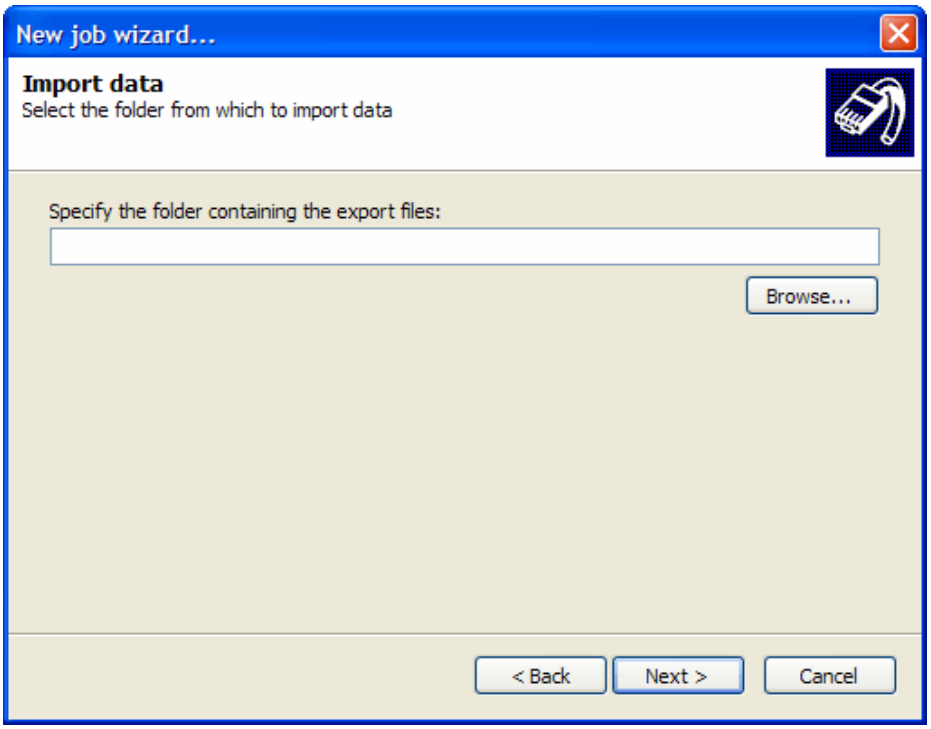
The following is an example of an export filename:

SERVER01_0051_20061020_20061025.EXP

12.7 Import from file

To import events from a file into the main database:

1. From the 'New job wizard' dialog, select the **Import from file** option.



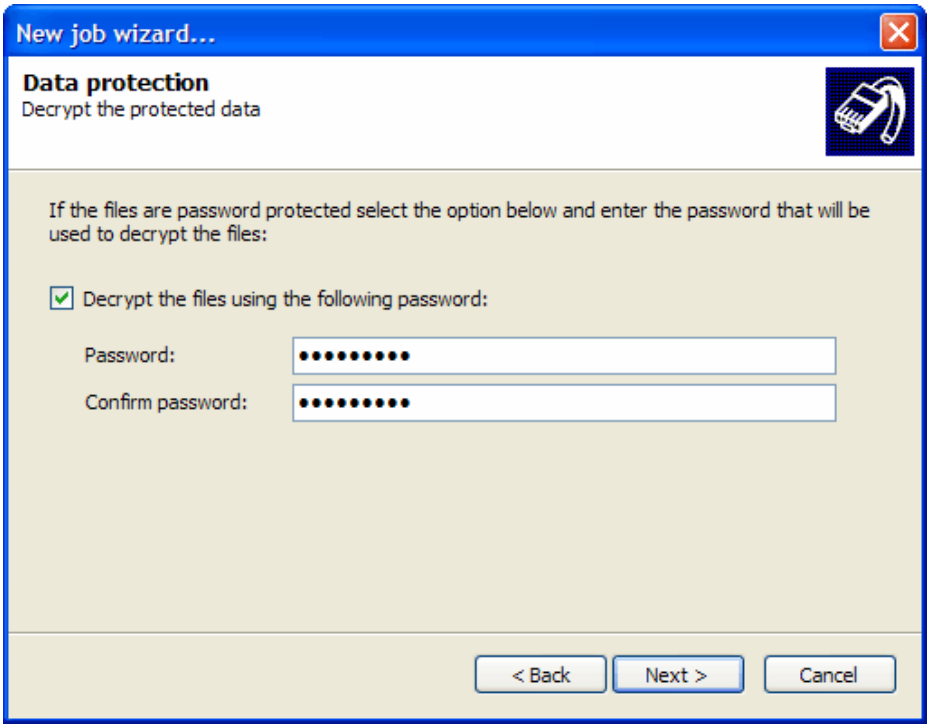
Screenshot 141 - New job wizard: Import from file

2. Specify the folder where the export file is stored. Use the UNC notation to specify remote paths.

NOTE 1: Ensure that GFI EventsManager has administrative privileges over the specified folder.

NOTE 2: GFI EventsManager will import all files having a .EXP extension.

3. Click **Next** to proceed to the data protection dialog.


New job wizard...
Data protection
Decrypt the protected data
If the files are password protected select the option below and enter the password that will be used to decrypt the files:
Decrypt the files using the following password:
Password:
Confirm password:
< Back
Next >
Cancel

Screenshot 142 - New job wizard: Import from file decryption

4. Specify the password with which events data will be decrypted and click **Next** to proceed to the data filter dialog.

NOTE: Use the same password used for the encryption of your events data.

5. Configure the data filters that will be applied against the imported file and click **Next** to continue.

NOTE 1: Use data filters to define which events will be imported into the main database.

NOTE 2: For more information on how to configure filter conditions, refer to the 'Configuring data filter conditions' section in this chapter.

6. Specify whether the maintenance job should be scheduled or executed immediately.

7. Click on **Finish** to finalize your settings.

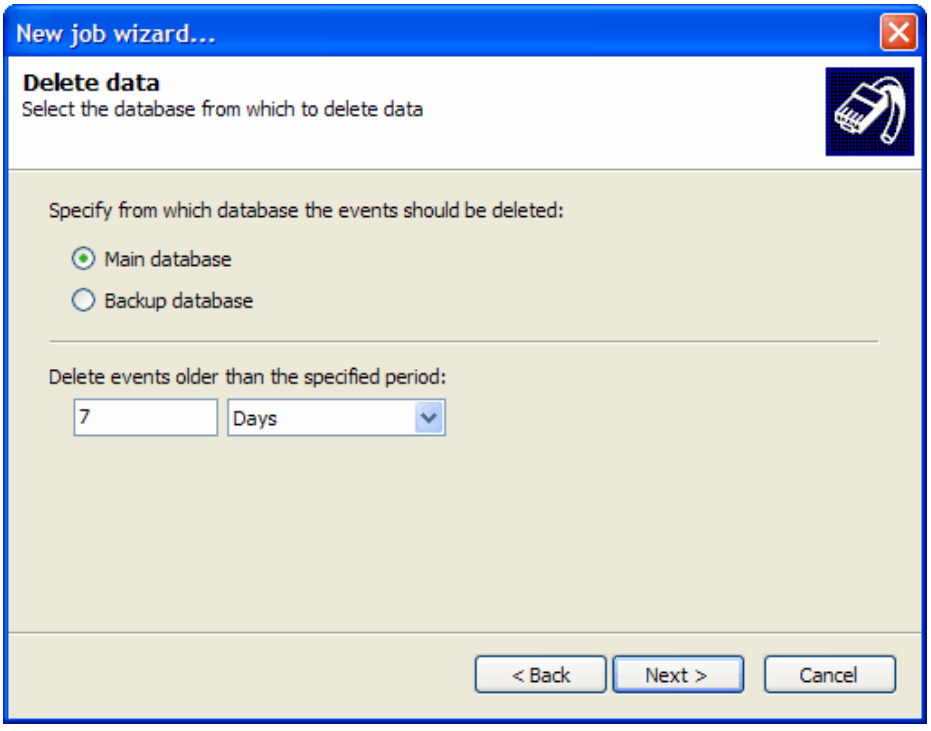
NOTE: GFI EventsManager will change the file extension of all successfully imported files from .EXP to .IMP.

12.8 Delete data

To remove events from the main database:

1. From the 'New job wizard' dialog, select the **Delete data** option.

NOTE: Important events data should be backed up through the 'Move to database' or 'Export to file' maintenance jobs. Failure to do this means that deleted records can NOT be recovered.



Screenshot 143 - New job wizard: Delete data

2. Specify whether events will be deleted from the Main database or from the Backup database.

3. Specify the frequency in hours/days at which events will be deleted from the main/backup database.

4. Click **Next** to bring up the data filter conditions dialog.

5. Configure the data filter conditions that will be applied for the 'Delete data' job. If you do not set any data filter conditions, than all events older than the specified period will be deleted. Click **Next** to continue.

NOTE: For more information on how to configure filter conditions, refer to the section 'Configuring data filter conditions' in this chapter.

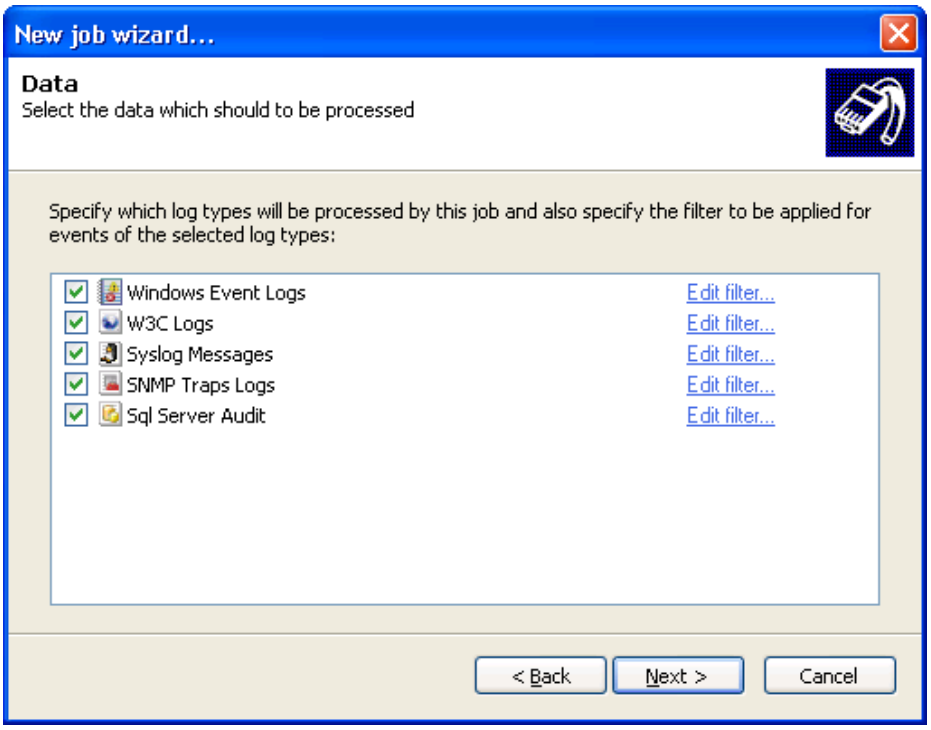
6. Specify whether the maintenance job should be scheduled or executed immediately.

7. Click on **Finish** to finalize configuration of the new 'Delete data' job.

12.9 Configuring data filter conditions

Use data filter conditions to specify which events will be affected by the maintenance job. Only events which match the specified criteria will be processed, moved, exported, deleted or imported.

- Filters can be created for all log types supported by GFI EventsManager.


New job wizard...
Data
Select the data which should to be processed
Specify which log types will be processed by this job and also specify the filter to be applied for events of the selected log types:
Windows Event Logs
W3C Logs
Syslog Messages
SNMP Traps Logs
Sql Server Audit
Edit filter...
Edit filter...
Edit filter...
Edit filter...
Edit filter...
< Back
Next >
Cancel

Screenshot 144 - Data filter dialog

To specify which events are affected by maintenance jobs, click on the **Filter** button in the data filter dialog. This dialog is available through the 'New job wizard'.

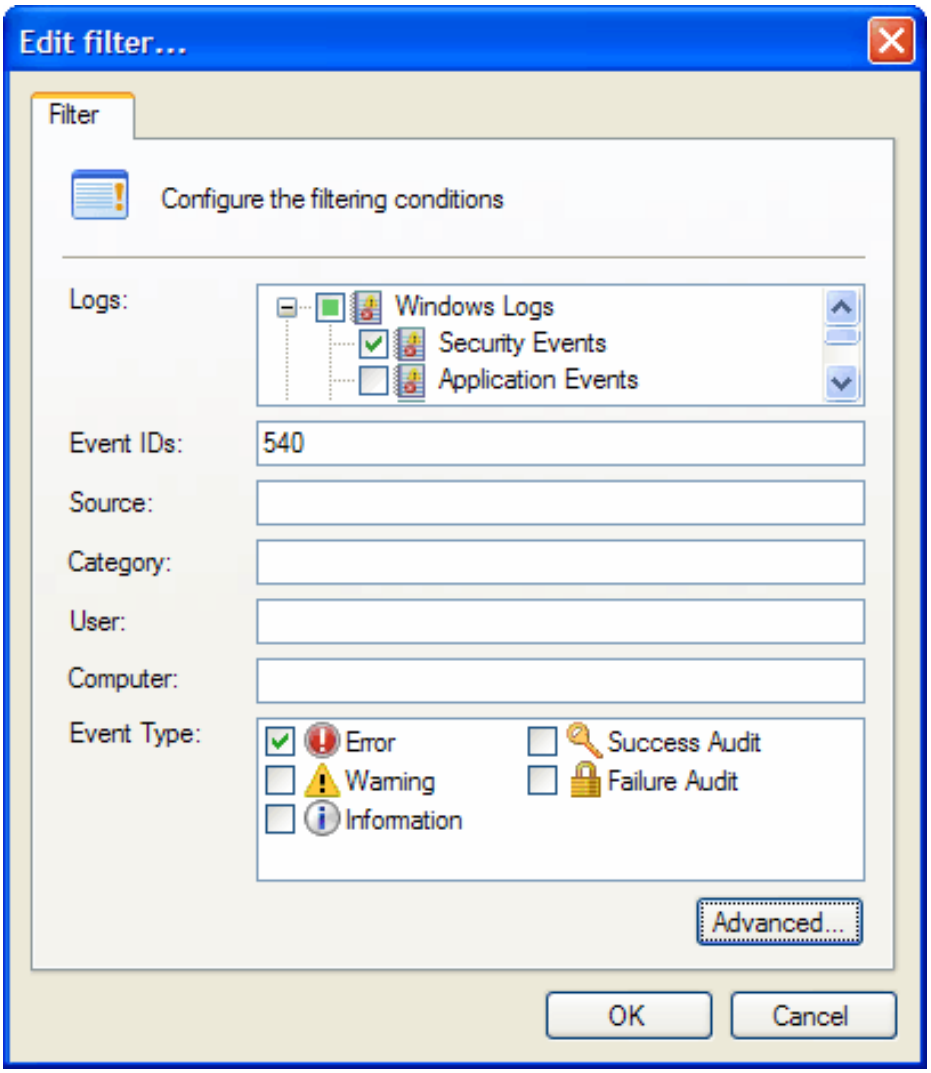
Example: Windows Event Log filter

Export events from the Windows Event Log with the following conditions:

- **Log type:** Security
- **Event ID:** 540 - Successful logon
- **User:** administrator

- **Event Type:** Error.

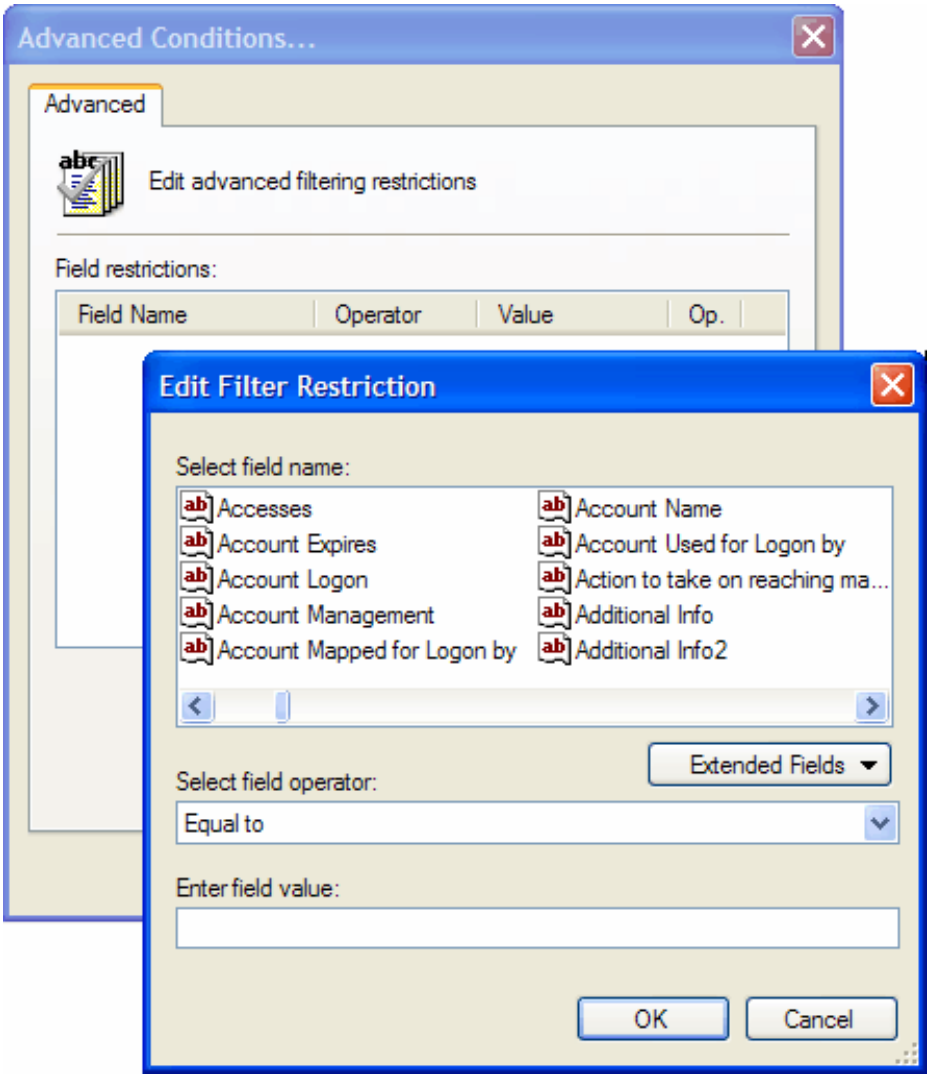
Configure your filter parameters as shown in the 'Edit filter' dialog shown below:



Screenshot 145 - Creating a filter for Windows events: Edit filter dialog

Click **Ok** to finalize filter configuration.

Advanced conditions

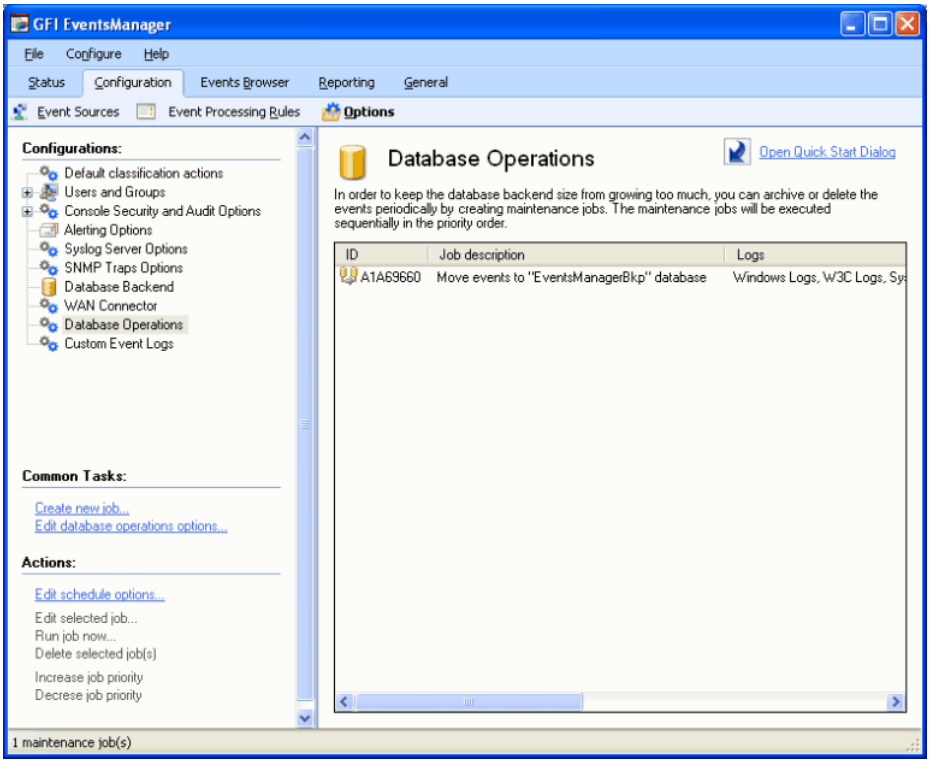


Screenshot 146 - Advanced Filter settings

From the 'Edit filter' dialog you can also set advanced filter conditions. Through this dialog you can also create and apply filters on all events data fields used by GFI EventsManager.

Note: Filters can also be applied on maintenance jobs after they have been created. For more information refer to the 'Editing a maintenance job' section.

12.10 Viewing scheduled maintenance jobs



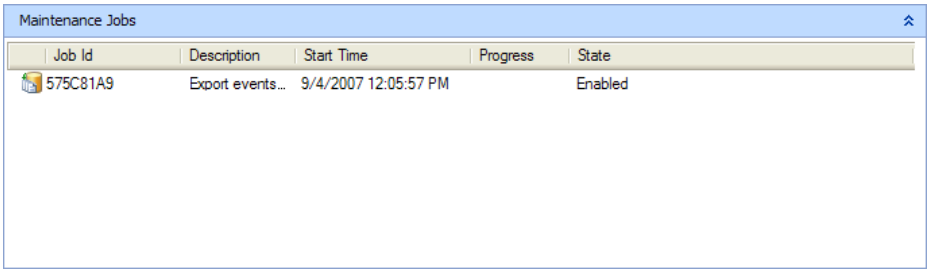
Screenshot 147 - Viewing scheduled maintenance jobs

To view maintenance jobs created:

1. Click on the **Configuration** tab and select **Options**.

2. From the left pane, select the **Database Operations** node. Scheduled maintenance jobs will be displayed in the right pane.

Job activity status



Screenshot 148 - Job activity status

To view the progress of maintenance jobs that are being processed click on the **Status** tab and select the **Job Activity** dashboard view. The status of all maintenance jobs will be displayed in the **Maintenance Jobs** section.

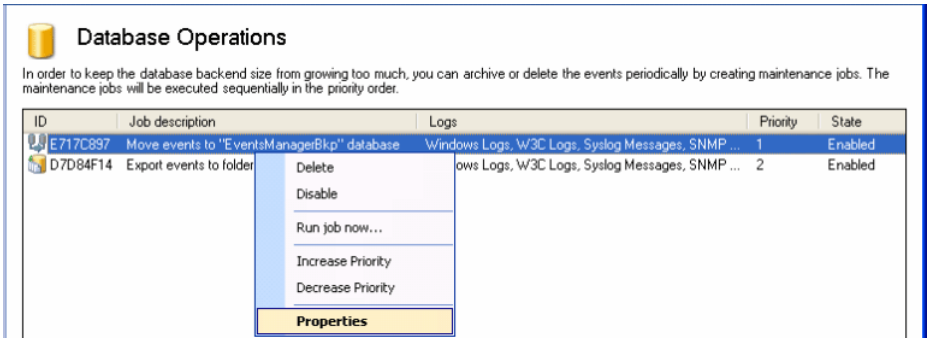
12.11 Editing a maintenance job

You can make changes to maintenance job parameters for jobs scheduled.

1. Click on the **Configuration** tab and select **Options**.

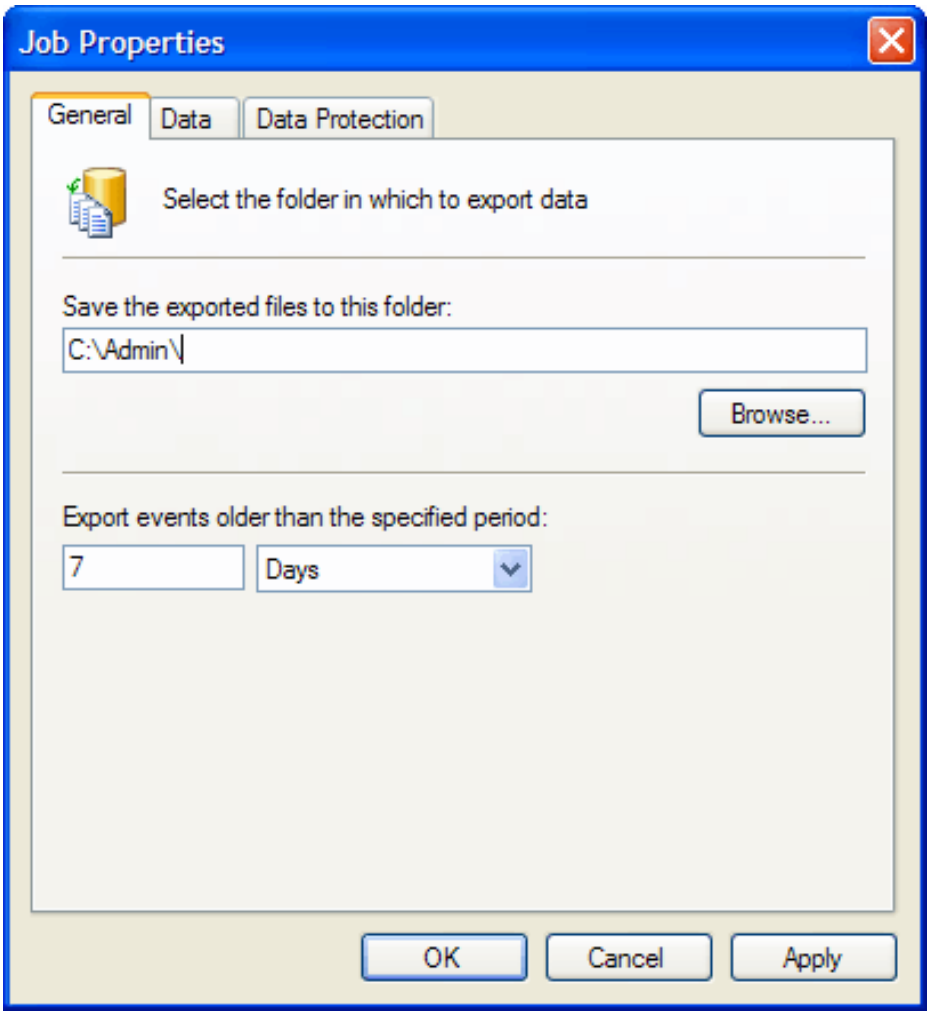
2. From the left pane, select the **Database Operations** node.

3. From the right pane, right-click on the maintenance job to edit and select **Properties**.



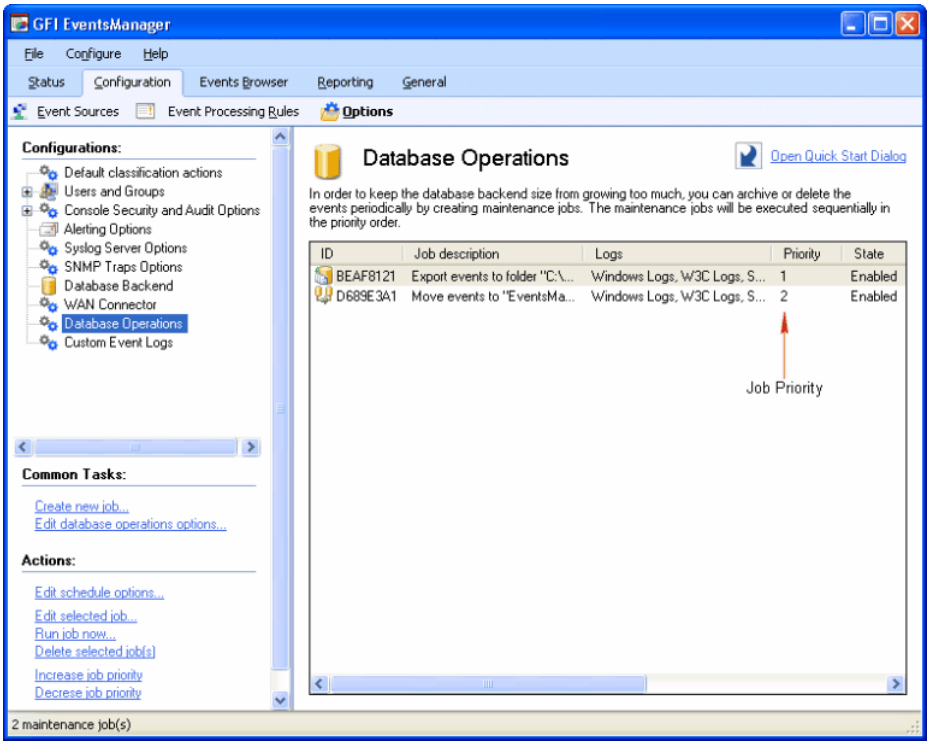
Screenshot 149 - Editing a maintenance job

4. Configure job properties and click **OK** to finalize your settings.



Screenshot 150 - Example dialog to edit a scheduled job

12.12 Changing maintenance job priority


GFI EventsManager
File Configure Help
Status Configuration Events Browser Reporting General
Event Sources Event Processing Rules Options
Configurations:
Default classification actions
Users and Groups
Console Security and Audit Options
Alerting Options
Syslog Server Options
SNMP Traps Options
Database Backend
WAN Connector
Database Operations
Custom Event Logs
Common Tasks:
Create new job...
Edit database operations options...
Actions:
Edit schedule options...
Edit selected job...
Run job now...
Delete selected job(s)
Increase job priority
Decrease job priority
Database Operations
Open Quick Start Dialog
In order to keep the database backend size from growing too much, you can archive or delete the events periodically by creating maintenance jobs. The maintenance jobs will be executed sequentially in the priority order.
ID Job description Logs Priority State
BEAF8121 Export events to folder "C:\... Windows Logs, W3C Logs, S... 1 Enabled
D689E3A1 Move events to "EventsMa... Windows Logs, W3C Logs, S... 2 Enabled
Job Priority
2 maintenance job(s)

Screenshot 151 - Maintenance job priorities

By default maintenance jobs are executed according to the sequence with which the jobs are created (First-in-First-out). Thus the priority of maintenance jobs is determined by the sequence in which jobs are executed.

To increase or decrease the priority of a maintenance job:

1. Click on the **Configuration** tab and select **Options**.

2. From the left pane, select the **Database Operations** node.

3. From the right pane, right-click on the maintenance job and select **Increase Priority** or **Decrease Priority** accordingly.

12.13 Deleting a maintenance job

Scheduled maintenance jobs awaiting execution can also be deleted.

1. Click on the **Configuration** tab and select **Options**.

2. From the left pane, select the **Database Operations** node.

3. From the right pane, right-click on the maintenance job to delete and select **Delete**.

IMPORTANT: Due diligence should be taken when deleting maintenance jobs for such an operation has an indirect effect on events data. An example is an 'Export to file' maintenance job with a higher priority than a 'Delete data' job. If you delete the 'Export to file' job, you end up with events data being removed without having any backup of such data.

13 Miscellaneous

13.1 Command line operations

GFI EventsManager provides you with three command line tools through which you can perform data export and import functions. These three tools are:

- Exportdata.exe: Exports data from an ESM 8 database using database operations engine
- Importdata.exe: Imports data into an EMS 8 database using database operations engine
- Importsettings.exe: Imports configuration from a data folder or from a configuration export file (.esmbkp) and is used mostly from installer when preserving configuration

Exportdata.exe

Use this tool to export data from the GFI EventsManager database to binary file.

Usage:

exportdata.exe <parameters list>

Parameter	Mandatory/ Optional	Description
/folder: <path & foldername>	Mandatory	Defines folder where the data file will be stored
/period: <number of hours>	Optional	Exports events older than the number of hours: Default = 7 days
/password: <file password>	Optional	Sets an encryption password
/delete	Optional	Deletes the events after export
/movetodb:<database name>	Optional	Moves the events to another database on the same server. If no name is specified, the backup database will be used

NOTE: Any parameter that contains spaces must be enclosed in double quotes (“).

Example:

Exportdata.exe /folder:c:\exportfiles /period:240 /password:aip112sK

Where data is exported with the following details:

- A folder called **exportfiles**, located at **c:**
- Data older than 10 days (**240hours**)
- Encrypt using password **aip112sK**

Importdata.exe

Use this tool to import data in binary files to the GFI EventsManager database.

Usage:

importdata.exe <parameters list>

Parameter	Mandatory/ Optional	Description
/folder:<path & foldername>	Mandatory	Defines folder where data file will be stored
/password:<file password>	Optional	Defines the password that will be used to decode files; if not specified, no password will be used
/dbserver:<databaseserver location >	Optional	Defines the database server where the destination database lies. If not specified, the database details specified in GFI EventsManager will be used.
/dbname:<database name>	Optional	Defines the destination database name. If not specified, the database name specified in GFI EventsManager will be used.
/dbuser:<username>	Optional	Defines the user name used to connect to database. If not specified, Windows authentication will be used.
/dbpass:<password>	Optional	Defines the password used to connect to destination server/database. If none is specified, password is ignored.

NOTE: Any parameter that contains spaces must be enclosed within double quotes (“).

Example:

importdata.exe /folder:c:\exportfiles /password:aip112sK /dbserver:192.168.3.55 /dbname:mainesmdb /dbuser:sa /dbpass:sapwd

Where data is imported with the following details:

- From folder called exportfiles, located at c:\
- Decrypted using password aip112sK
- Saved to database on server with I.P. address 192.168.3.55, with database name: mainesmdb and with the following login credentials: username: sa and password sapwd.

Importsettings.exe

Use this tool to import GFI EventsManager configurations previously exported.

Usage:

importsettings.exe <parameters list>

Parameter	Mandatory /Optional	Description
/operation:<operation>	Mandatory	Defines the operation to perform, either importfolder or import file
/destination:<destination path>	Optional	Defines the destination folder where the configuration will be imported
/Sourcefile:<filename>	Optional	Defines the name of the file that contains the exported GFI EventsManager configuration.
/Sourcefolder:<folder name/path>	Optional	Defines the name of the folder that contains the exported GFI EventsManager configuration.

NOTE: Any parameter that contains spaces must be enclosed in double quotes (“).

Example:

importdata.exe /operation:importfolder: /destination: c:\esm\data /sourcefolder: c:\esm\old /

Where data is imported with the following details:

- Operation is **importfolder** to c**:\esm\data** from folder **c:\esm\old**

Customizing unique identifiers

GFI EventsManager enables you to customize the unique identifiers of the GFI EventsManager installation. This enables you to import the same configuration into separate without incurring duplicate GFI EventsManager instance IDs.

To configure new GFI EventsManager unique identifiers add the following option to command line options of importdata.exe

Parameter	Mandatory/ Optional	Description
/id:<new_id>	Optional	Defines the new ESM instance id set after importing the configuration. Use this parameter on only if you only want to change the ESM instance id; if no value is specified the existing ESM instance id will be preserved.

13.2 Product licensing

For information on GFI EventsManager licensing refer to:

http://www.gfi.com/page/13789/products/gfi-eventsmanager/pricing/licensing/licensing

13.2.1 View license details

To check your licensing details:

1. Click on the **General** tab.

2. From the left pane, click on the **Licensing** option. Licensing details will be displayed in the right pane of the management console.

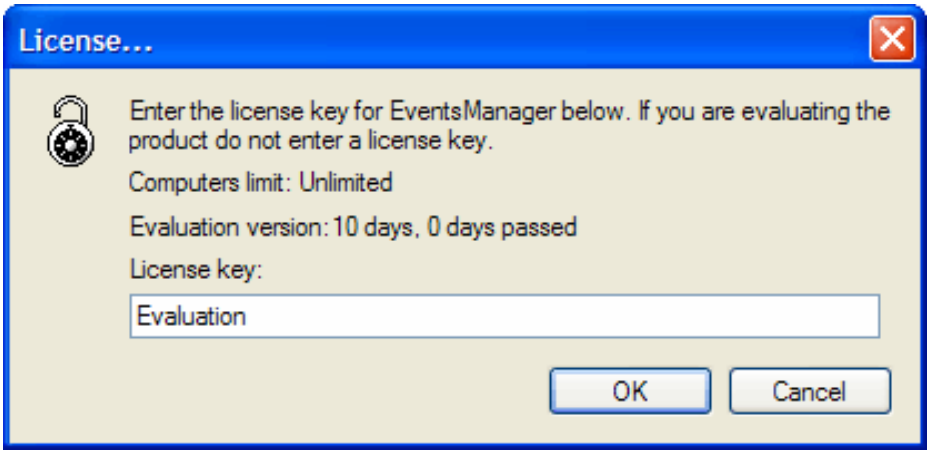
3. To view license distribution details click on **Show Details**. This will show the number of event sources configured and respective license type (i.e. Workstation or Server).

13.2.2 Update license key

To enter your license key after installation:

1. Click on the **General** tab.

2. From the left pane, right-click on the **Licensing** option and select **Edit license key…**


License...
Enter the license key for EventsManager below. If you are evaluating the product do not enter a license key.
Computers limit: Unlimited
Evaluation version: 10 days, 0 days passed
License key:
Evaluation
OK
Cancel

Screenshot 152 - Update license key

3. Specify your license key details.

4. Click **OK** to finalize your settings.

13.2.3 Update license type

To change the type of license allocated to a specific event source:

1. Bring up the (computer/computer group) properties dialog and click the **Licensing Type** tab

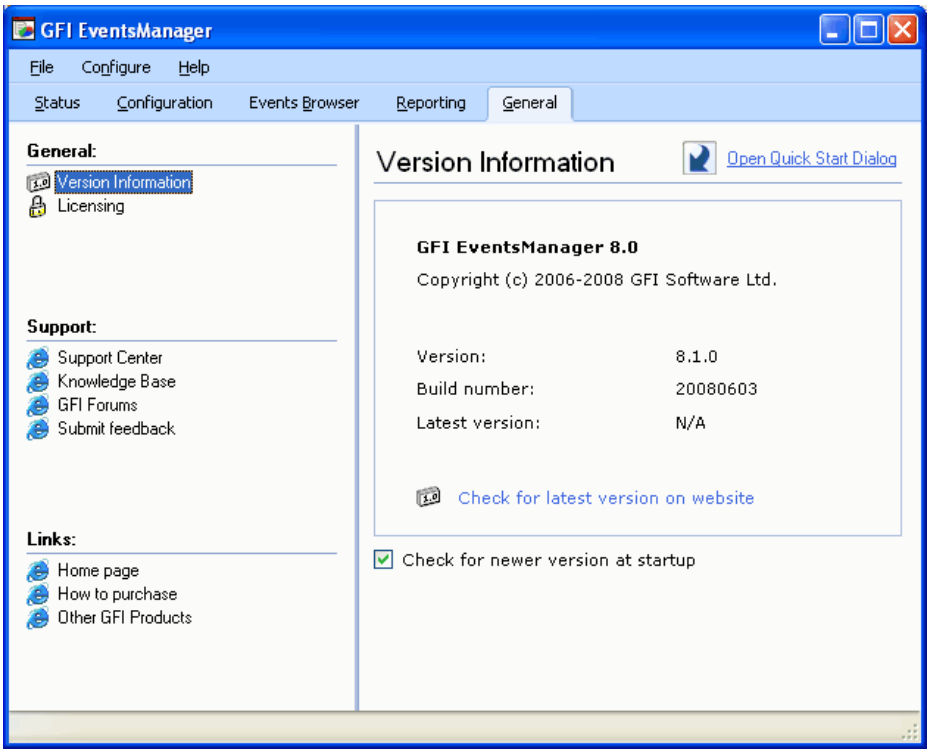
2. By default event sources inherit their licensing type from parent group (i.e. use the license type configured in parent group properties). To change license type select the Server License or Workstation option accordingly.

13.3 Version information

To check your version information details:

1. Click on the **General** tab.

2. Click the **Version Information** option. The version information details will be displayed in the right pane.



Screenshot 153 - Version Information screen

13.3.1 Checking for newer builds

To check for newer builds of GFI EventsManager:

1. Click on the **General** tab.

2. From the left pane, right-click on the **Version Information** option and select **Check for newer builds…**

14 Troubleshooting

14.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- The manual - most issues can be solved by reading this manual.
- GFI Knowledge Base articles
- Web forum
- Contacting the GFI Technical Support

14.2 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit http://kbase.gfi.com/.

14.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: http://forums.gfi.com/.

14.4 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online:** Fill out the support request form on: http://support.gfi.com/supportrequestform.asp. Follow the instructions on this page closely to submit your support request.
- **Phone:** To obtain the correct technical support phone number for your region please visit: http://www.gfi.com/company/contact.htm.

NOTE: Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

14.5 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: http://www.gfi.com/pages/productmailing.htm.

Index

A

actions 1, 2, 6, 9, 55, 56, 57, 72, 80, 83, 85, 87, 89, 90, 91, 93, 94, 95, 96

B

backup events 39, 40

D

database backend 1, 6, 9, 23, 33, 39, 40, 72

Database Operations 7, 121, 124, 125, 126, 127, 128, 130

default alerting settings 96

Demilitarized Zone 12, 13

DNS server 13, 19, 58

E

email alerts 2, 55, 93, 95, 97, 100

environment 14

event archiving 2, 72, 93

event classification 6, 56, 72, 93, 94

event color-coding 32

event finder tool 33

event processing rules 3, 5, 6, 9, 55, 60, 63, 65, 70, 72, 73, 75, 93, 95

event query 6, 30, 31, 33, 34

event query builder 6, 34, 39

event sources 5, 8, 9, 26, 44, 45, 48, 60, 63, 80, 82, 85, 87, 89

events browser 1, 29

EventsManagerAdministrator 101, 102, 103

export events to CSV 4, 30, 33, 39

F

filter conditions 130, 131, 133, 135, 136

I

installation wizard 15

L

License type 146

licensing 10, 15, 145

logon credentials 48

M

Management Information Base 7

N

network alerts 2, 93, 95, 98, 103

noise 9, 56, 75

O

operational time 45, 48, 49, 80, 82, 85, 87, 89

P

privileges 15

Q

Quick Start Dialog 23

R

rule-set 72, 73, 75, 76, 77, 78, 80, 83, 85, 87

S

scanning monitor 115

SMS alerts 2, 3, 95, 99, 100

SNMP Traps 1, 2, 3, 4, 9, 14, 22, 29, 49, 68, 69, 70, 71, 75, 85, 87, 117, 119, 120, 122, 123

SQL Server audit 7, 12, 29, 51, 55, 75, 87

Syslog messages 3, 9, 12, 13, 21, 64, 65, 67, 83

Syslog server 21, 64, 65, 66, 68, 70

U

upgrading 14

V

version information 146

W

W3C logs 3, 8, 19, 20, 55, 62, 80, 81, 90

WAN Connector 7

Windows Event Logs 3, 5, 8, 19, 46, 55, 57, 59, 62, 72, 73, 75

working hours 1, 48, 49, 79, 80, 82, 85, 87, 89, 102, 104, 105